HP StorageWorks

HA-Fabric Manager user guide

FW 08.01.00/HAFM SW 08.08.00

Part number: AA-RS2CG-TE
Sixth edition: December 2005

Legal and notice information

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

Linux is a U.S. registered trademark of Linus Torvalds.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Printed in the US.

HA-Fabric Manager user guide

Contents

Figures

Tables

About this guide

This guide provides information about:

- Using the High Availability Fabric Manager (HAFM) to monitor, configure, and manage the Fibre Channel in which managed products operate.
- Managing fabric zoning and HAFM logs.

Intended audience

This guide is intended for use by data center administrators, LAN administrators, operations personnel, and customer support personnel who:

- Administer user access to the HAFM application.
- Monitor and manage product operation.

Related documentation

For a list of corresponding documentation, see the related documents section of the release notes that came with the product.

For the latest information, documentation, and firmware releases, see the following StorageWorks web site:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, see the Fibre Channel Association web site: http://www.fibrechannel.org

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

💡 **TIP:** Provides helpful hints and shortcuts.

Rack stability

⚠ **WARNING!** To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, secure racks together.
- Extend only one rack component at a time. Racks can become unstable if more than one component is extended.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls can be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site at http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-345-1518.
- Elsewhere, visit the HP web site: http://www.hp.com. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For third-party product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com

1 HAFM overview

HAFM is a graphical user interface (GUI) that enables you to manage users and products, monitor products, and open Element Managers.

This chapter describes the following topics:

- HAFM components, page 21
- SAN life cycle, page 24
- Searching the online help, page 25
- System requirements, page 26

HAFM components

The HAFM application is installed on the 1U rack-mount appliance (HAFM appliance) to provide local access to managed products. HAFM client applications can also be installed on remote user workstations to provide remote access to the managed products through the HAFM appliance. Figure 1 shows an example of an HAFM configuration.

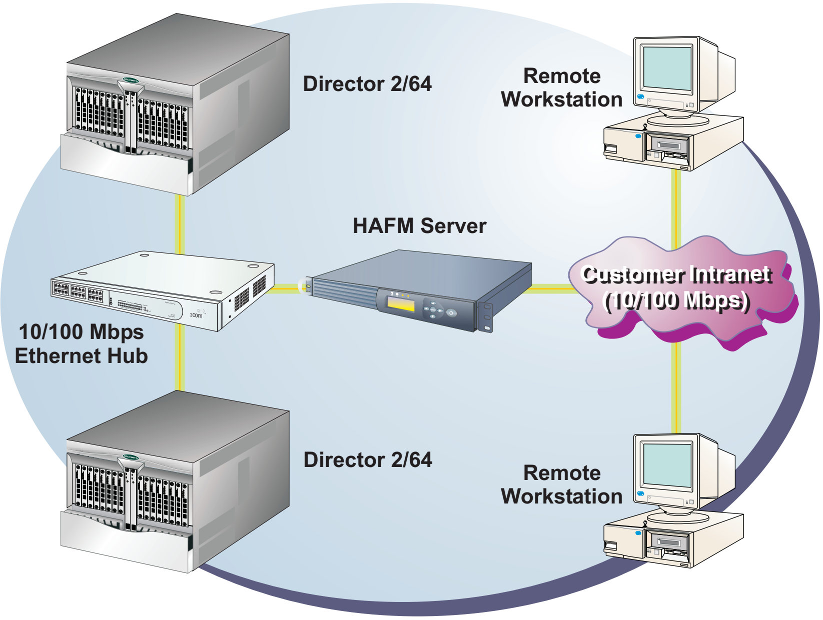


Figure 1 Product management options

HAFM appliance

The HAFM appliance provides a central point of control for managed Fibre Channel products. The HAFM appliance is required for installing, configuring, and managing these products.

See the *HP StorageWorks HA-Fabric Manager installation guide* for details about the HAFM appliance.

NOTE: Although products can perform normal operations without an HAFM appliance, the HAFM appliance should operate at all times to monitor product operations, report failures, log event changes, and log configuration changes.

HAFM application

The application is composed of two parts: the *appliance* (which runs only on the HAFM appliance) and the *client*. The server is installed on one HAFM appliance and stores storage area network (SAN) information; it does not have a user interface. To view SAN information through a user interface, you must log in to the server running on the appliance through a client.

NOTE: The server and clients can reside on the same machine or on separate machines.

In most configurations, the server calls the client whenever it has new data.

In some cases, a network can utilize virtual private network (VPN) or firewall technology, which can prohibit communication between the server application running on HAFM appliances and clients. In this situation, the application automatically detects the network configuration and runs the client in *polling mode*. See "Configuring HAFM through a firewall" on page 195.

Dual LANs on the HAFM appliance

When two LANs are connected at the HAFM appliance, Microsoft® Windows® and the HAFM application designate one as the public LAN, and the other as the private LAN.

- The private LAN is for communication between the HAFM appliance and the directors and edge switches that the HAFM appliance manages.
- The public LAN is for communication between the HAFM appliance and computers seeking remote client access to the HAFM appliance.

Either LAN connection on the HAFM appliance can be the public LAN or the private LAN. The directors and edge switches can be managed via either LAN; however, only the public LAN supports remote client access.

The title bar of the main window of the HAFM application shows the IP address of the public LAN.

Public and private LAN designations

In a dual LAN configuration, both LANs must be connected when the HAFM appliance boots. If only one is connected, the HAFM appliance interprets this as a single LAN configuration, and the connected LAN is designated as the public LAN.

The HAFM application designates the public LAN as the first LAN detected whose IP address is not the reserved private subnet 10.x.x.x. Thus, if neither IP address is 10.x.x.x, the first LAN detected by the HAFM application is designated as the public LAN. This order of detection is influenced by Microsoft Windows and not guaranteed.

There are a two ways to ensure the pubic and private designations of the LANs:

- Assign the private LAN IP address, 10.x.x.x, to the LAN you want designated as the private LAN. You must also have the public LAN connection active when the HAFM appliance is booting up.
- Configure a specified Ethernet interface on the HAFM appliance to be the public LAN by manually editing a file on the HAFM appliance to explicitly specify which IP address the HAFM application should use as the public LAN.

  Perform the following to configure an Ethernet interface:

  - Open the `config.properties` file in directory `C:\Program Files\HAFM\`, and add the following line:

    ```
    ServerRmiIpAddress=x.x.x.x
    ```

    where *`x.x.x.x`* is the IP address assigned to the Ethernet LAN adapter which is to be used as the public LAN. This entry is case sensitive and must be made exactly as shown. After this line has been added, reboot the HAFM appliance.

NOTE: Rebooting the server does not impact the Fibre Channel operations of any edge switch or director. Only monitoring switch operations, logging events, and implementing configuration changes are interrupted.

Remote access to the public LAN

If the public LAN IP address of the HAFM appliance is changed, you must edit the `config.properties` file to reflect the new IP address.

Remote workstations are not supported on the secondary adapter, and must always connect to the public adapter.

For details on configuring remote workstations, see "Configuring remote workstations" on page 257.

Out-of-band access

Besides the HAFM application and Element Managers on the HAFM appliance, out-of-band (non-Fibre Channel) management access to HP directors and switches is provided through the following:

- A Simple Network Management Protocol (SNMP) agent implemented through the HAFM application. Administrators on SNMP management workstations can access product management information using any standard network management tool. Administrators can assign IP addresses and corresponding community names for up to 12 SNMP workstations functioning as SNMP trap message recipients.
- The Internet, using the HAFM Basic interface installed on the director or switch. This interface supports configuration, statistics monitoring, and basic operation of the product, but does not offer all the capabilities of the corresponding Element Manager in HAFM. Administrators launch the web server interface from a remote PC by entering the product's IP address as the Internet URL, and then entering a user name and password at a login window. The PC browser then becomes a management console.
- A PC-based Telnet session using the command line interface (CLI). Any platform that supports Telnet client software can be used.

SAN life cycle

The HAFM application enables you to proceed through the four stages of the managed life cycle of the SAN with confidence. Table 2 describes the different stages in the life cycle.

At any point, a discovered SAN can be used as a starting point to plan a new SAN, completing the life cycle.

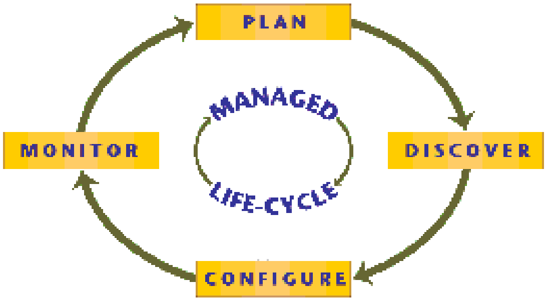


Figure 2 SAN life cycle

Table 2 Stages of a SAN life cycle

Stage	Task	Description
1	Plan the SAN	The administrator uses paper and pen or a software application to plan the SAN.
2	Discover the SAN	The HAFM application establishes contact with many SAN devices, gathers embedded information, and presents a visual map of devices and their connections as a Physical/Topology map.
3	Configure the SAN	The administrator configures SAN devices and fabrics.
4	Monitor the SAN	The self-monitoring, event-logging, and event notification application generates events and messages about product and property status. The user interface features an animated display of the data flow and error rates over the entire topology.

Searching the online help

To find help topics that contain a particular word or phrase:

1. On the Help window, click the tab with the magnifying-glass icon.
2. In the Find box, enter the word or phrase for which you want to search.
3. Press **Enter**.

If any matches are found, a list of topics is displayed in the panel. The number of times the word or phrase occurs in the topic is displayed next to the name.

4. Click the name to display that topic.

System requirements

This section describes client and server system requirements for HAFM.

HAFM appliance system requirements

The server running the HAFM application must meet the following requirements for Windows or Solaris platforms. When setting up your HAFM appliance:

- Use the recommended configuration.
- To set up Call Home, follow the steps in "Configuring Call Home for remote dial-in" on page 62.
- To backup, follow the steps in "Customer-supplied server backup" on page 58.

NOTE: A maximum of eight clients are allowed per HAFM appliance.

NOTE: The HAFM appliance supports up to 48 HP directors or switches (managed products).

Table 3 Windows system hardware requirements for HAFM

	Minimum	**Recommended**
Processor	2.0 GHz Intel® Pentium® 4 Processor	3.0 GHz, 1 MB/800 MHz FSB Intel Pentium 4 Processor
Hardware	24/8X CD-RW/DVD Combo, Data Only	48/32X CD-RW/DVD Combo, Data Only
Operating system	Windows 2000®, service pack 4	Windows 2003 Server Standard Edition
Memory	1 GB	2 GB, DDR400 SDRAM Memory
Graphics card	16 MB	32 MB, VGA capable
Hard drive	40 GB	40 GB ATA-100 IDE (7200 rpm)
Modem	56K, v.92 data/fax modem, PCI	56K, v.92 data/fax modem, PCI
Ethernet NIC	10/100 Mbps Ethernet LAN card	10/100 Mbps Ethernet LAN card

Table 4 Windows system requirements for HAFM

Processor	1 GHz Intel Pentium III or greater
Hardware	CD-RW
Operating system	Windows 2000 Professional, service pack 4 Windows 2003® Windows XP®, service pack 1 Windows 2000 Server, service pack 4 Windows 2000 Advanced Server, service pack 4
Memory	1 GB RAM (minimum)
Disk space	650 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors

Table 5 Solaris system requirements for HAFM

Processor	400 MHz Solaris UltraSparc II or greater
Hardware	CD-ROM
Operating system	Solaris 7, Solaris 8, or Solaris 9
Memory	512 MB RAM (minimum)
Disk space	650 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors
Network interface adapter	Supporting TCP/IP

NOTE: HAFM for Solaris (HAFM Lite) includes all of the features of HAFM except for the Call Home and Backup features.

HAFM client system requirements

The client system running HAFM must meet the following requirements:

NOTE: A maximum of eight clients is allowed per HAFM appliance.

Table 6 Windows system requirements

Processor	1 GHz Intel Pentium III or greater
Hardware	CD-ROM
Operating system	Windows 2000 Professional with service pack 3 or greater Windows 2003
Memory	1 GB RAM (minimum)
Disk space	350 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors

Table 7 Solaris system requirements

Models	Ultra 10 or greater
Processor	UltraSparcIli or greater
Hardware	CD-ROM
Operating system	Solaris 8 or 9
Memory	512 MB RAM (minimum)
Disk space	350 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors

Table 8 Linux system requirements

Processor	1 GHz Intel Pentium III and greater
Hardware	CD-ROM
Operating system	Red Hat Enterprise Linux® ES 3.0 Red Hat 9.0 kernel v.2.4.20-8 Red Hat 8.0 kernel v.2.4.18-14
Memory	512 MB RAM (minimum)
Disk space	350 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors

Table 9 HP-UX system requirements

Models	9000/785/B2000
Processor	400 MHz PA-RISC
Hardware	CD-ROM
Operating system	HP-UX version 11.0
Memory	512 MB RAM (minimum)
Disk space	350 MB disk space
Video requirements	HP VISUALIZE-FXE color, 1280x1024 48 planes
Resolution	256 colors

Table 10 AIX system requirements

Model	RS/6000 44P Model 170
Processor	333 MHz Power3-II
Hardware	CD-ROM
Operating system	AIX 5.1
Memory	512 MB RAM (minimum)
Disk space	350 MB disk space
Video requirements	8 MB video RAM
Resolution	256 colors

2 Using the HAFM application

This chapter provides instructions for using the HAFM application. The following topics are described:

- Managing the appliance, page 31
- Viewing the HAFM main window, page 33
- Accessing the HAFM application, page 36
- Monitoring the HAFM application, page 40
- Using the Group Manager, page 43
- Configuring nicknames, page 48
- Exporting and importing data, page 51
- Backing up and restoring data, page 56
- Accessing to Eclipse management applications, page 60

Managing the appliance

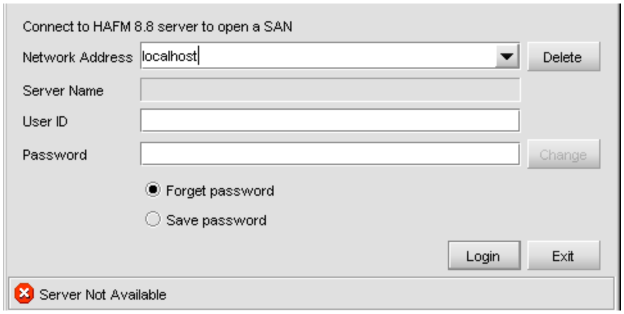
This section describes how to add, remove, log in to, and log out of the HAFM appliance.

Logging in to HAFM

You must log in to a appliance to monitor a SAN.

NOTE: You must have a login and password account on the HAFM appliance in order to log in.

1. The HAFM Log In dialog box is displayed automatically when you open HAFM (Figure 3).



Connect to HAFM 8.8 server to open a SAN

Network Address localhost

Server Name

User ID

Password

● Forget password

○ Save password

Server Not Available

Figure 3 HAFM Log In dialog box

The HAFM appliance address is displayed in the Network Address box.

2. You can specify a new address by typing it in the box, or selecting one from the list.

NOTE: Localhost is the default. HAFM determines the local IP address and uses it to log in.

3. The HAFM appliance name is displayed in the Server Name box.
4. Enter your user ID and password.
5. Select whether you want the application to remember your password the next time you log in.
6. Click **Login**.

Logging out of HAFM

To log in to a different HAFM appliance, you must first log out of the current appliance.

1. Select **SAN > Log Out**.

   The HAFM Log In dialog box is displayed (Figure 3 on page 31).

You are logged out of the appliance and the HAFM Log In dialog box is displayed (Figure 3).

Adding an appliance

1. Select **SAN > Log Out**.

   The HAFM Log In dialog box is displayed (Figure 3 on page 31).
2. To add a new appliance, enter the appliance network address in the Network Address box.

TIP: If the appliance and client are on the same machine, you can type **localhost** in the Network Address box.

NOTE: You must have an established login and password account on the new appliance.

   The appliance name is displayed in the Server Name box.
3. Enter your user ID and password.
4. Specify whether you want the application to remember your password the next time you log in.
5. Click **Login**.

   The application logs in to the appliance located at the specified network address.

Removing an appliance

You can remove appliances from the list in the Log In dialog box.

1. If you are logged in to an appliance, select **SAN > Log Out**. If you do not have the application open, start the application.

   The HAFM Log In dialog box is displayed (Figure 3 on page 31).
2. Select the appliance you want to remove from the Network Address list.

   The selected appliance IP address is displayed in the Network Address box.

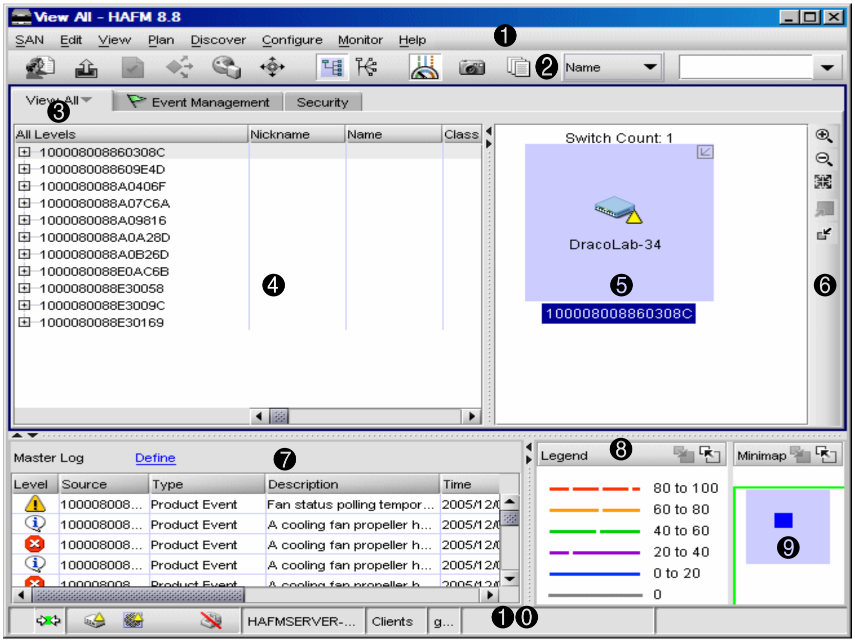
IMPORTANT: The appliance will be deleted without confirmation.

3. Click **Delete**.
4. Click **OK**.

Viewing the HAFM main window

Figure 4 shows the View All display of the HAFM main window. You can customize your window view to show only the information that you need (see "Creating a customized view" on page 83).

NOTE: Some panels can be hidden by default. To view all panels, select **View > All Panels** or press **F12**.



All Levels	Nickname	Name	Class
⊞ 100008008860308C			
⊞ 1000080088609E4D			
⊞ 1000080088A0406F			
⊞ 1000080088A07C6A			
⊞ 1000080088A09816			
⊞ 1000080088A0A28D			
⊞ 1000080088A0B26D			
⊞ 1000080088E0AC6B			
⊞ 1000080088E30058			
⊞ 1000080088E3009C			
⊞ 1000080088E30169			

Level	Source	Type	Description	Time
⚠	100008008...	Product Event	Fan status polling tempor...	2005/12/(
ℹ	100008008...	Product Event	A cooling fan propeller h...	2005/12/(
✖	100008008...	Product Event	A cooling fan propeller h...	2005/12/(
ℹ	100008008...	Product Event	A cooling fan propeller h...	2005/12/(
✖	100008008...	Product Event	A cooling fan propeller h...	2005/12/(

1 Menu bar
2 Toolbar
3 View tab
4 Product List
5 Physical/Topology map
6 Toolbox
7 Master log
8 Connection utilization legend
9 Minimap
10 Status bar

Figure 4 View All - HAFM window

HAFM main window panels

This section describes each panel of the HAFM main window.

Menu bar

The menu bar (Figure 4 ❶) consists of pull-down menus that allow you to view information, and configure and manage the application.

Toolbar

The toolbar (Figure 4 ❷) provides buttons to perform various functions. Place your cursor on a toolbar button for information about the button function.

NOTE: Depending on your configuration, the buttons on your toolbar can differ from the example.

View tab

The View tab (Figure 4 ❸) displays the Master Log, Physical Map (topology), and Product List. Change the default size of the display by placing the cursor on the divider until a double arrow is displayed. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

Product List

The Product List (Figure 4 ❹) shows an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses. To display the Product List, select Product List from the View menu, or press F9. You can edit information in the Product List by double-clicking in a box marked with a green triangle. You can sort the Product List by clicking a column heading. See "Customizing the Product List" on page 86 for information about customizing the information displayed in the Product List.

Physical/Topology map

The Physical/Topology map (Figure 4 ❺) shows devices and their connections and ports. A topology is a logical and/or physical arrangement of devices on a network. See "Creating a customized view" on page 83 for information about customizing the information displayed in the Physical/Topology map.

Toolbox

The toolbox (Figure 4 ❻) allows you to vary the window display, and generate Physical Map reports. Place your cursor on a toolbox icon for information about its function.

Master log

The Master log (Figure 4 ❼) lists the events that occurred on the SAN. The default locations for the log files are:

- `Install_Home\Server\Universe_Home\Test Universe \_Working\EventStorageProvider\event.log`
- `Install_Home\Server\Local_Root\EventStorageProvider\event.log`

Connection utilization legend

The connection utilization legend (Figure 4 ❽) shows the percentage of utilization on the trunks on the Physical Map. The color and length of the lines indicate the bandwidth utilization.

Minimap

The Minimap (Figure 4 ❾) provides a high-level view of the entire SAN. You can use it to navigate to more detailed map views. This feature is especially useful if you have a large SAN. To quickly jump to a specific place on the Physical Map, click the corresponding area on the Minimap.

Anchoring or floating the Minimap

You can anchor or float the Minimap to customize your main window.

Floating the Minimap

To float the Minimap and view it in a separate window, click **Detach** in the upper right-hand corner of the Minimap.

Anchoring the Minimap

To return the Minimap to its original location on the main window, do one of the following:

- Click **Attach** in the upper right-hand corner of the Minimap.
- Click **Close** in the upper right-hand corner of the Minimap.
- Click the logo in the upper left-hand corner of the Minimap and click **Close (Alt - F4)**.

Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow is displayed. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow is displayed. Click and drag to change the window size.

Status bar

The status bar (Figure 4 ❶⓿) provides status information about the SAN and the application. Place your cursor on a status bar icon for information about the status displayed. The icons are:

- **Server Status**—Displays local appliance status.
- **Connection Status**—Displays the appliance-client connection status.
- **Product Status**—Displays the most degraded status of all devices in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status is displayed as degraded. Click this button to open the Product State Log. See "Determining the operational status" on page 80 for more information.
- **Fabric Status**—Displays the state of the fabric that is least operational, based on ISL status. The possible states are:
  - Operational
  - Unknown
  - Degraded
  - Failed

Select a product or fabric from the Physical Map or Product List and click this button to open the related Fabric Log (only available for persisted fabrics). See "Monitoring events" on page 101 for more information.

- **Attention Indicator**—Displays when at least one HP product in the SAN has an attention indicator. Click the icon to open the Service Request dialog box, which lists all HP switches and directors that need attention.
- **Call-Home Status**—Displays the Call Home status if the Call-Home service has been enabled. If Call-Home has been enabled on all managed HP switches and on the management application, the icon is displayed as enabled. If Call-Home is disabled on any one of the HP switches or on the management application, the icon is displayed as disabled. Click the icon to open the Call Home Settings Summary dialog box, which indicates whether the Call-Home feature is enabled on HAFM and on each managed HP switch or director.
- **Server Name**—Displays the name of the appliance to which you are connected.
- **Client Count**—Displays the number of clients.
- **User's Access Level**—Displays the user ID of the logged-in user.

NOTE: Depending on your configuration, the icons on your status bar can differ from the example.

Selecting a customized view of the main window

See "Creating a customized view" on page 83 to specify which information you want to display on the main window. To select a customized view, click the **View** tab and then select the view name from the menu.

Accessing the HAFM application

You can access the HAFM application in one of two ways:

- Log in from a local, browser-capable PC connected through an Ethernet LAN segment.
- Log in remotely with an HAFM client application.

Accessing the HAFM application locally

You can log in to the HAFM application located on the HAFM appliance from a PC connected through an Ethernet LAN segment:

1. Launch the browser application (Netscape Navigator or Internet Explorer) from the PC.
2. Enter the URL in the following format:

   ```
   http://xxx.xxx.xxx.xxx:5800
   ```

   xxx.xxx.xxx.xxx is the default IP address or the IP address configured for the appliance during installation.

The VNC Authentication window is displayed (Figure 5).

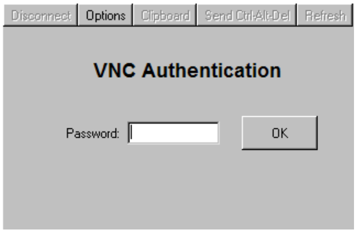
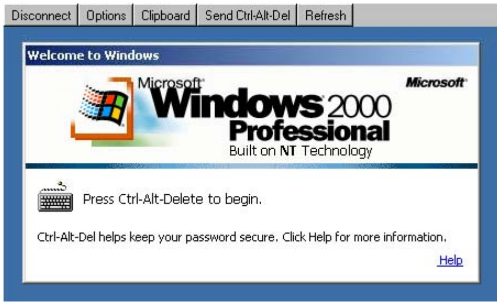


Figure 5 VNC Authentication window

3. Enter the password and click **OK**.

   The Welcome to Windows dialog box is displayed (Figure 6).

NOTE: The default VNC viewer password is `password`.



Press Ctrl-Alt-Delete to begin.

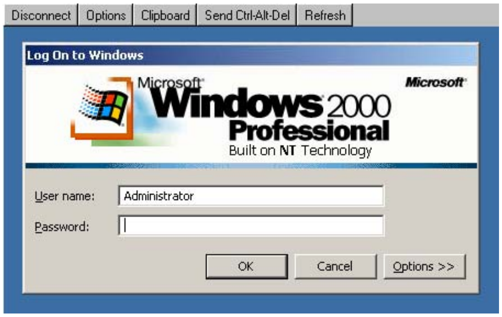
Ctrl-Alt-Del helps keep your password secure. Click Help for more information.

Figure 6 Welcome to Windows dialog box

4. Click **Send Ctrl-Alt-Del** at the top of the window to log on to the HAFM appliance desktop.

   The Log On to Windows dialog box is displayed (Figure 7).

NOTE: Do not press **Ctrl-Alt-Delete** on your keyboard. This logs you on to the PC instead of the HAFM appliance.



User name: Administrator

Password:

Figure 7 Log On to Windows dialog box

5. Enter the Windows 2000 user name and password and click **OK**.

   You are logged in to the PC and the desktop is displayed.

NOTE: The default Windows 2000 user name is `Administrator` and the default password is `password`. The user name and password are case sensitive.

6. If the HAFM 8.8 Log In dialog box is not displayed, double-click the HAFM 8.8 icon on the desktop.

   The HAFM 8.8 Log In dialog box is displayed (Figure 3 on page 31).

   The default address that is displayed in the Network Address box is the address of the last appliance accessed. Click the Network Address list to view the network addresses of all HAFM appliances that were accessed from the computer you are logged in to.

7. Enter the HAFM appliance IP address in the Network Address box.
   - If you want to connect to an HAFM appliance on the list, select the IP address.
   - If you are logging in to the local HAFM appliance, the network address is `localhost`.
   - If you want to connect to an HAFM appliance that is not listed, enter the IP address.

8. Enter your user name and password in the User ID and Password boxes, respectively.

NOTE: If user names have not been established, use the default user name `Administrator` and password `password`. HP recommends that you change the default password as soon as possible.

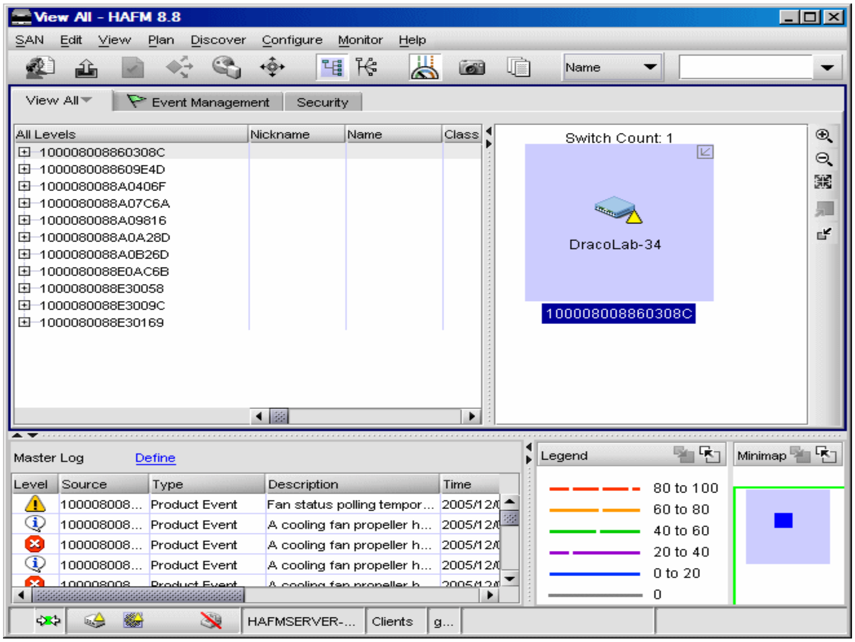
   To add or modify user names, passwords, and user rights, see "Managing users" on page 63.

9. If you want your computer to save the login information, select **Save Password**.

10. Click **Login**.

    The HAFM window is displayed (Figure 8 on page 39).

The network address you entered remains in the Network Address list for future logins. If you fail to connect to the appliance, the HAFM window is not displayed and the network address does not remain in the list.



All Levels	Nickname	Name	Class
⊞ 100008008860308C			
⊞ 1000080088609E4D			
⊞ 1000080088A0406F			
⊞ 1000080088A07C6A			
⊞ 1000080088A09816			
⊞ 1000080088A0A28D			
⊞ 1000080088A0B26D			
⊞ 1000080088E0AC6B			
⊞ 1000080088E30058			
⊞ 1000080088E3009C			
⊞ 1000080088E30169			

Master Log Define

Level	Source	Type	Description	Time
⚠	100008008...	Product Event	Fan status polling tempor...	2005/12/
ⓘ	100008008...	Product Event	A cooling fan propeller h...	2005/12/
✖	100008008...	Product Event	A cooling fan propeller h...	2005/12/
ⓘ	100008008...	Product Event	A cooling fan propeller h...	2005/12/
✖	100008008	Product Event	A cooling fan propeller h	2005/12/

Figure 8 HAFM window

Accessing the HAFM application remotely

Users at remote PCs can access the HAFM application and Element Managers loaded on the appliance if the following criteria are met:

- The remote workstation meets minimum hardware and software requirements (see "Configuring remote workstations" on page 257).
- The HAFM client application is running. If you need to install the HAFM client application, see "Configuring remote workstations" on page 257.
- The remote system is configured to connect with the HAFM appliance over a TCP/IP network connection.
- No more than seven other remote users are currently logged in to the HAFM application.

Operators at remote workstations can manage and monitor all products controlled by the HAFM appliance. Each active connection between a remote workstation and an HAFM appliance and managed product is called a session.

To access the HAFM appliance from a remote workstation, perform the following:

1. If the HAFM application is not running or the HAFM 8.8 Log In dialog box is not displayed on your remote workstation, start the client application by following the appropriate procedure for your workstation's operating system (see Table 11):

Table 11 Starting HAFM on a remote workstation

Operating software	**Procedure**
Windows 2000 Windows NT Windows XP	**a.** Start the HAFM client application using one of the following options: • Select **Start > Programs > HP HAFM > HAFM x.x**. • Double-click the HAFM x.x desktop icon. **b.** Enter the network address, user ID, and password for the HAFM appliance you want to access. **c.** Click **Login**. The HAFM client accesses the HAFM appliance, and the View All - HAFM window is displayed (Figure 8).
HP-UX AIX Linux Solaris	From the directory in which you installed the HAFM application (usually the home directory): **a.** Go to the location where you installed the application (the default is `/usr)`. **b.** Start the appliance and client: `./HAFM` **c.** To start the client only: `./Client` Or Go to the `bin` directory in which you installed the application (the default is `/opt/`): `cd /`*`path`*`/HAFM `*`x.x`*`/bin` **d.** Start the appliance: `./HAFM_Mgr start` **e.** Start the client: `./HAFM_Client`

2. Click **OK**.
3. Follow step 7 through step 10 in "Accessing the HAFM application locally" on page 36.

Logging out of an appliance

To log out of the appliance select **SAN > Log Out**.

You are logged out of the current appliance and the HAFM 8.8 Log In dialog box is displayed (Figure 3 on page 31).

Monitoring the HAFM application

This section describes monitoring the HAFM application.

Starting and stopping HAFM Services

HAFM Services is the software application that provides services to the HAFM application. HAFM Services runs only on the HAFM appliance.

You can start or stop HAFM Services from the desktop:

1. Select **Start > Programs > HP StorageWorks ha-fabric manager 8.8 > Stop Services**.
   Or
   Select **Start > Programs > HP StorageWorks ha-fabric manager 8.8 > Start Services**.

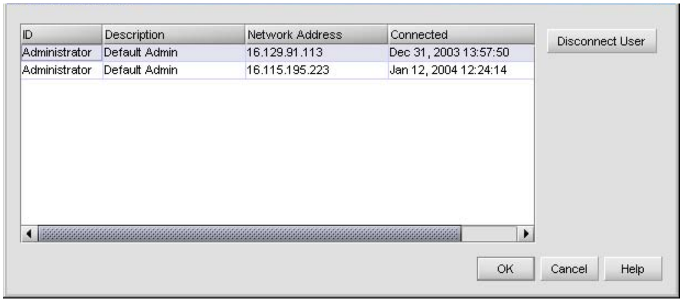
Viewing user sessions

Monitoring clients is an important part of maintaining the SAN because more than one client can access an appliance at a time. You can view user sessions to determine which clients are logged in to the appliance.

To display the Active Sessions dialog box:

1. Select **SAN > Active Sessions**.

   The Active Sessions dialog box is displayed (Figure 9).



ID	Description	Network Address	Connected
Administrator	Default Admin	16.129.91.113	Dec 31, 2003 13:57:50
Administrator	Default Admin	16.115.195.223	Jan 12, 2004 12:24:14

Figure 9 Active Sessions dialog box

The Active Sessions dialog box shows information about the active users. If a user is logged in from more than one location, there is a separate entry for each session.

Disconnecting users

To disconnect a user:

1. Select a user and click **Disconnect User** to disconnect the user from the appliance.

   The appliance immediately shuts down the appliance-client connection. The status bar on the client displays that the appliance connection was lost. All products and connections on the Physical Map stay in the condition they were in when the session ended; they do not turn grey. The client displays a message stating that a user disconnected the client from the appliance.

NOTE: To prevent this user from reconnecting, remove the user account. See ”Removing a user account” on page 65 for instructions.

Fibre Channel networks use World Wide Names (WWNs) to uniquely identify nodes and ports within nodes. For many devices, the 64-bit WWNs are fixed, and their assignment follows conventions established by the IEEE. For other devices, the WWNs can be set or modified by the user. WWNs are a special concern for SAN Manager because:

- WWNs are used as the primary keys to identify network elements.
- Previous experiences have shown that an ill-formed WWN can be a malfunctioning device.

Proper operation with SAN Manager requires that WWNs be unique within the network and well-formed (they must be 64 bits in length and the first byte cannot be zero).

Determining user groups

An administrator can determine the groups to which a user belongs:

1. Select **SAN > Users**.

   The Server Users dialog box is displayed (Figure 26 on page 64).
2. Select a user from the Users table.
3. Click **Find**.

   The groups to which the user belongs are highlighted in the Groups list.
4. Click **OK**.

Determining the discovery state

NOTE: The Product List panel can be hidden by default. To view the Product List, select **View > Product List** or press **F9**.

You can determine the discovery status of products by looking at the status column in the Product List. Table 12 lists the operational statuses and their equivalent discovery states.

Table 12 Discovery state equivalent

Operational status	Discovery state
Unknown	Offline
Operational Degraded Failed	Online

Grouping on the Physical Map

To simplify the Physical Map, devices are displayed in groups (Figure 10). Groups are displayed with background shading and are labeled as a group. You can expand and collapse groups to easily view a large topology.

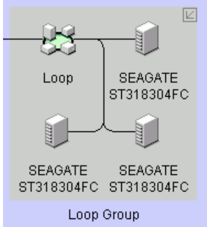


Figure 10 A group on the Physical Map

NOTE: Zonable fabrics are true fabrics. Fabric groups are a set of connected devices that can or cannot be fabric devices.

Collapsing groups

To collapse a single group on the Physical Map:

- Double-click the icon at the top right corner of the group on the topology ( ).
- Double-click in the group, but not on a device.
- Right-click in a group, but not on a device, and select **Collapse**.

To collapse all groups on the topology by one level, click the Collapse icon on the HAFM toolbox ( ).

Expanding groups

To expand a group on the Physical Map:

- Double-click the group icon.
- Right-click the group icon and select **Expand**.

To expand all groups on the topology by one level, click the Expand icon on the HAFM toolbox ( ).

Using the Group Manager

The Group Manager allows you to make changes related to the configuration and monitoring of switches and directors. This function also allows you to make changes to multiple devices at the same time. You can:

- Install firmware on switches and directors.
- Initiate data collections on multiple switches.
- Create group event logs.

When you launch Group Manager for the first time, the **Select Action** tab is selected with the following options available:

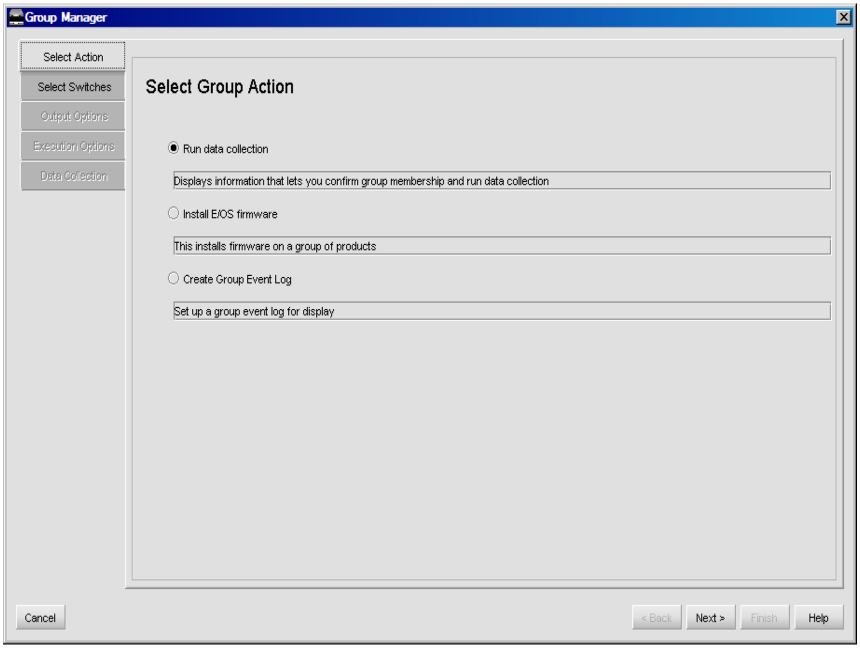
- Run data collection
- Install E/OS firmware
- Create Group Event Log

Select Action tab with Run data collection selected

To access Group Manager:

1. Select **Configure > Group Manager**.

   The Group Manager dialog box is displayed (Figure 11).
2. Select **Run data collection** and the following tabs are displayed on the left-side:
   - Select Action
   - Select Switches
   - Output Options
   - Execution Options
   - Data Collection



Select Group Action

● Run data collection

Displays information that lets you confirm group membership and run data collection

○ Install E/OS firmware

This installs firmware on a group of products

○ Create Group Event Log

Set up a group event log for display

Figure 11 Select Group Action dialog box

Select Action tab with Install E/OS firmware selected

The Install E/OS firmware option installs firmware on a group of products.

1. Select **Configure > Group Manager**.

   The Group Manager dialog box is displayed (Figure 11 on page 44).

2. Select **Install E/OS firmware** and the following tabs are displayed on the left-side:
   - Select Action
   - Select Switches
   - Select Firmware
   - Execution Options
   - Install
   - History

Select Action tab with Create Group Event Log selected

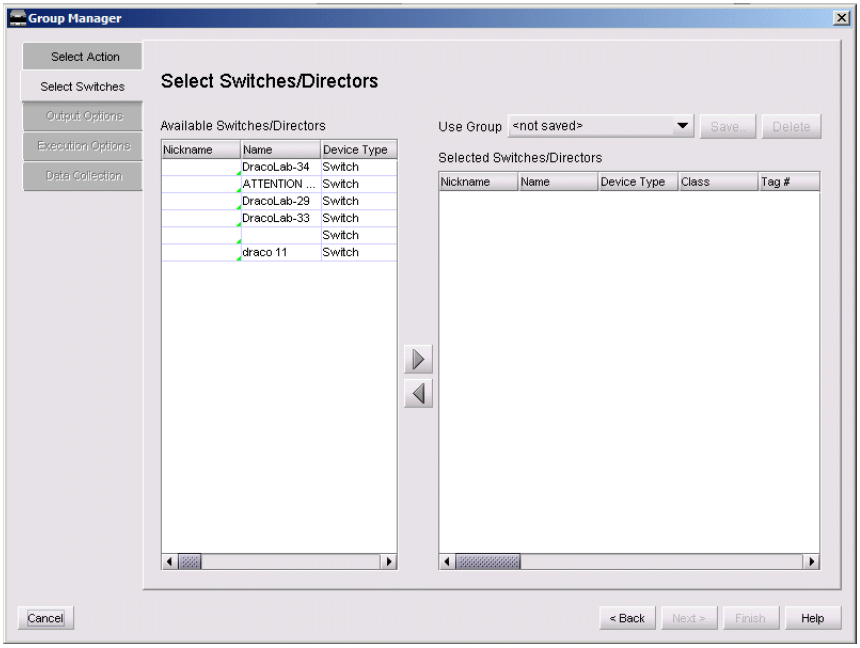
1. Select **Configure > Group Manager**.

   The Group Manager dialog box is displayed (Figure 11 on page 44).

2. Select **Create Group Event Log** and the following tabs are displayed on the left-side:
   - Select Action
   - Select Switches
   - Create Log

Displaying the Select Switches tab

The Select Switches tab displays all switches and directors discovered by the HAFM appliance and allows you to select any set of those products for use in the Group Manager.



Select Switches/Directors

Available Switches/Directors

Nickname	Name	Device Type
	DracoLab-34	Switch
	ATTENTION ...	Switch
	DracoLab-29	Switch
	DracoLab-33	Switch
		Switch
	draco 11	Switch

Use Group <not saved>

Selected Switches/Directors

Nickname	Name	Device Type	Class	Tag #

Figure 12 Select Switches tab

Select switches and directors in the Available Switches/Directors table and move them to the Selected Switches/Directors table or to remove them from the Selected list using the arrows.

Select the Use Group list to select a group and the table is populated with the products in the group. To add a group, move a switch or director from the Available Switches/Directors table to the Selected Switches/Directors table. Click **Save,** type a group name, and then click **OK**.

Displaying other tabs

- **Select Firmware**—Displays all firmware that can be installed on any product in the selected products list. Use this tab to add, revise, and delete firmware.
- **Output Options**—Displays the output options information where you can save all data collections files to a folder. You can also save the data collections files in a single zipped file.
- **Execution Options**—Displays execution options information. You can pause before executing the action on each product or halt the process anytime an error occurs.
- **Data Collection**—Displays data collection options information that lets you confirm group membership and run data collection.
- **Install**—Displays install information that lets you confirm group membership and install firmware.
- **History**—Displays history information of firmware installations. Select the product firmware install that you want to reverse.
- **Create Log**—Confirms group membership and creates a log of that information.

Using the Group Log

The Group log lets the user view, delete, or export the event logs defined on the Group Manager window. To access this log:

1. Select **Monitor > Logs > Group**.

   The Group Log is displayed.
2. Click **Delete Log** if you want to delete the log.

   A confirmation message dialog box is displayed.

   a. Click **OK**.
3. Click **Export** if you want to export the log.

   The Save Group Logs dialog box is displayed.

   a. Enter the name of file.

   b. Click **OK**.

Viewing detail on the Product List

You can view different levels of information on the Product List.

Viewing all details

To display all information on the Product List:

1. Click **View All**.
2. Select **Levels > All Levels**.

To display only products on the Product List:

1. Click **View All**.
2. Select **Levels > Products Only**.

Zooming in and out of the Physical Map

You can zoom in or out of the Physical Map to view products and ports.

Zooming in

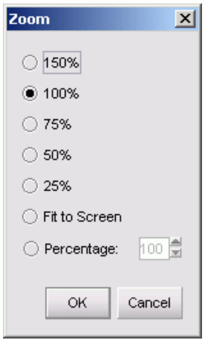
To zoom in on the Physical Map, use one of the following methods:

1. Click the zoom-in icon (🔍) on the HAFM toolbox.

   or

   Select **View > Zoom**.

   The Zoom dialog box is displayed (Figure 13).



Zoom

○ 150%

● 100%

○ 75%

○ 50%

○ 25%

○ Fit to Screen

○ Percentage: 100

Figure 13 Zoom dialog box

2. Select a zoom percentage.
3. Click **OK**.

Zooming out

To zoom out of the Physical Map, use one of the following methods:

1. Click the zoom-out icon (🔍) on the toolbox.

   or

   Select **View > Zoom.**

   The Zoom dialog box is displayed (Figure 13).
2. Select a zoom percentage.
3. Click **OK**.

Changing view options on the Physical Map

To change the view of the Physical Map, select **View > Show** from the HAFM menu bar, and then select one of the available view options.

Turning flyovers on or off

Flyover text is displayed when you place the cursor on a product. They provide a quick way to view a product's properties.

To turn flyovers on or off:

1. Select **View > Enable Flyover Display** and select the check box to enable flyovers.
   Or
   Select **View > Enable Flyover Display** and deselect the check box to disable flyovers.

Configuring nicknames

HAFM allows you to use nicknames as a method of providing simple names to products and ports in a SAN. Using HAFM you can:

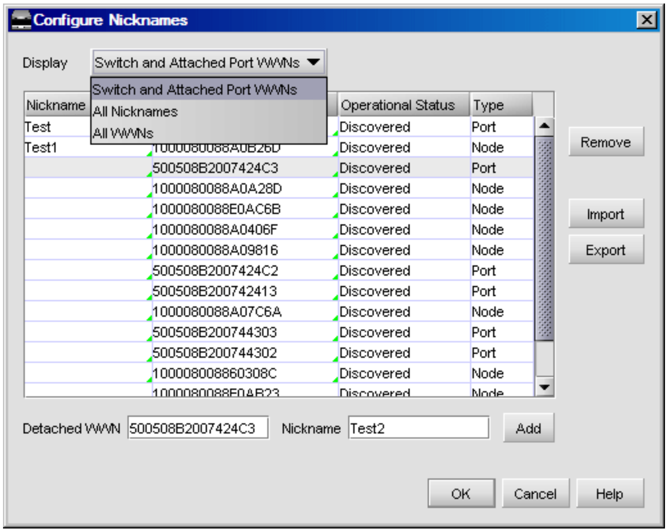
- Associate a nickname with a product or port WWN that has been discovered.
- Add a WWN and an associated nickname for a product or port that has not yet been discovered.
- Remove or disassociate a nickname from a WWN.

Viewing nicknames

You can view devices by the device nickname.

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14).



Display: Switch and Attached Port WWNs

Nickname		Operational Status	Type
Test		Discovered	Port
Test1	1000080088A0B26D	Discovered	Node
	500508B2007424C3	Discovered	Port
	1000080088A0A28D	Discovered	Node
	1000080088E0AC6B	Discovered	Node
	1000080088A0406F	Discovered	Node
	1000080088A09816	Discovered	Node
	500508B2007424C2	Discovered	Port
	500508B200742413	Discovered	Port
	1000080088A07C6A	Discovered	Node
	500508B200744303	Discovered	Port
	500508B200744302	Discovered	Port
	100008008860308C	Discovered	Node
	1000080088E0AB23	Discovered	Node

Detached WWN: 500508B2007424C3 Nickname: Test2

Figure 14 Configure Nicknames dialog box

2. Using the Display list, specify how you want to display devices:
   - Select **All Nicknames** to display all devices with a nickname.
   - Select **All WWNs** to display all discovered devices with a WWN.

- Select **Switch and Attached Port WWNs** to display all devices.

The table displays the nickname, WWN, operational status, and type of the device.

Assigning a nickname to an existing device

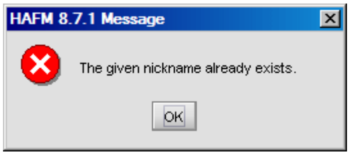
To assign a nickname to an existing device:

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14).
2. Select **All WWNs** from the Display list.

   All discovered devices are displayed.
3. Double-click in the Nickname column of the device that to which you want to assign a nickname.
4. Enter the nickname for the device and press **Enter**.

   If the nickname you entered already exists, the following message is displayed (Figure 15).



The given nickname already exists.

Figure 15 Nickname already exists message

   a. If you entered a duplicate nickname, click **OK** and go back to step 3.

5. Click **OK**.

Adding a nickname to a new device

To add a nickname to a new device:

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14 on page 48).
2. Enter the WWN of the device in the Detached WWN box.
3. Enter the nickname for the device in the Nickname box.
4. Click **Add**.

   The new device and nickname is displayed.
5. Click **OK**.

Importing nicknames

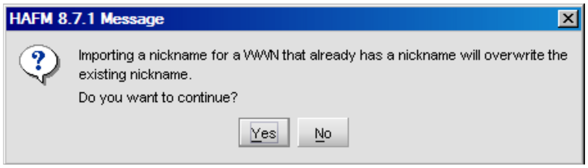
This section describes how to import nicknames from the Configure Nicknames dialog box. You can also import nicknames from the Import dialog box. For more information, see "Importing data" on page 55.

To import nicknames:

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14 on page 48).
2. Click **Import**.

A confirmation message is displayed (Figure 16).


HAFM 8.7.1 Message

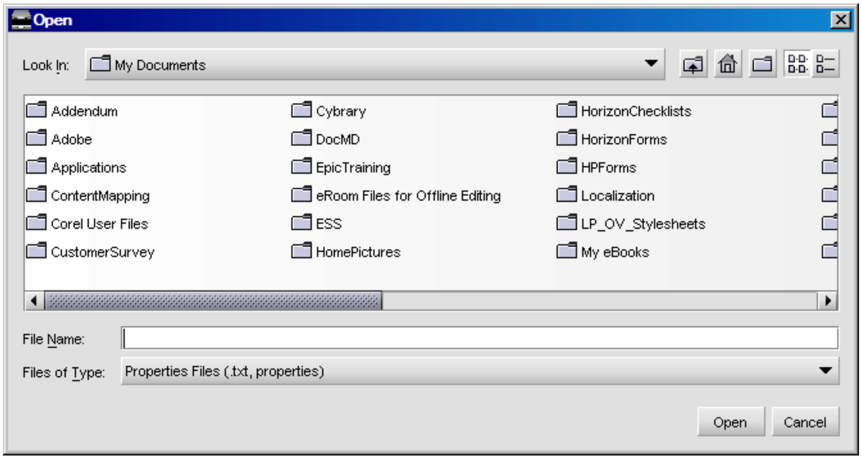
Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname.

Do you want to continue?

Figure 16 Import nicknames confirmation message

3. Click **Yes** to continue.

   The Open dialog box is displayed (Figure 17).


Open

Look In: My Documents

File Name:

Files of Type: Properties Files (.txt, properties)

Figure 17 Open dialog box

4. Browse to file you want to import and then click **Open**.

   The file is imported and assigned.

5. Click **OK**.

Exporting nicknames

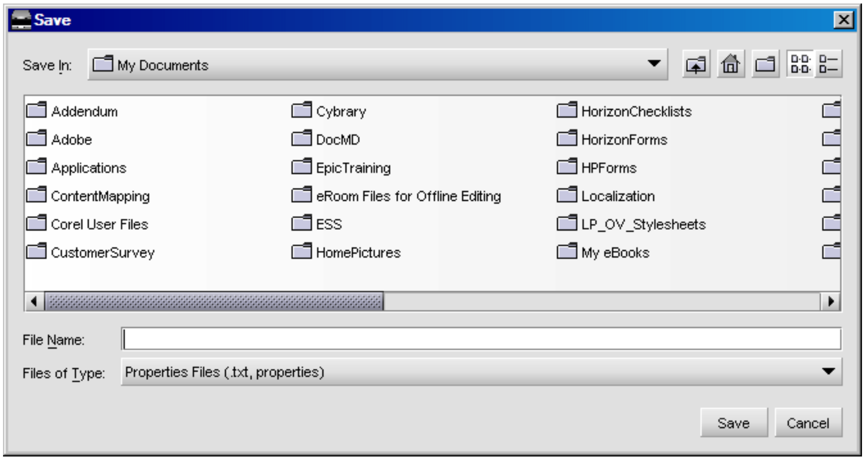
To export a nickname:

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14 on page 48).

2. Select **All Nicknames** or **All WWNs** from the Display list.
3. Click **Export**.

The Save dialog box is displayed (Figure 18).



Save In: My Documents

File Name:

Files of Type: Properties Files (.txt, properties)

Figure 18 Save dialog box

4. Browse to the folder where you want to save the file and enter a file name in the File Name box.
5. Click **Save**.

   The file is exported to the selected folder.

Removing a nickname

To remove a nickname:

1. Select **Configure > Nicknames**.

   The Configure Nicknames dialog box is displayed (Figure 14 on page 48).
2. Select the nickname of the device you want to remove.
3. Click **Remove**.

   A confirmation message is displayed.
4. Click **Yes**.
5. Click **OK**.

Exporting and importing data

The import and export features are important functions of the application. You can import and export data for many reasons, including to communicate issues to the support center and to capture network status.

NOTE: Currently, you can only export to and import from the same version of HAFM application (for example, export from 08.06.00 and import to 08.06.00).

Importing a file imports the following:

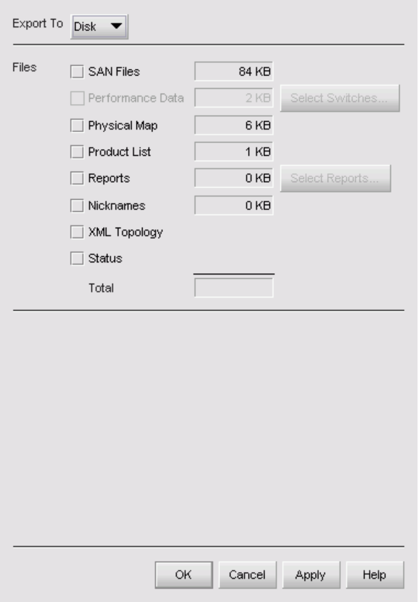
- Physical map

- Status icons
- User properties
- Discovered properties as they were set at the time of the export

Exporting data

To export data to disk or e-mail:

1. Select **SAN > Export**.
   The Export Discovered SAN dialog box is displayed (Figure 19).



Export To: Disk

Files

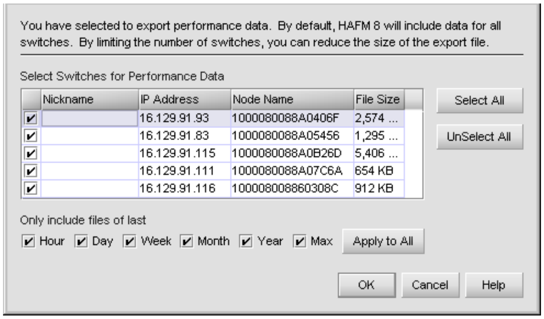
□ SAN Files	84 KB	
□ Performance Data	2 KB	Select Switches...
□ Physical Map	6 KB	
□ Product List	1 KB	
□ Reports	0 KB	Select Reports...
□ Nicknames	0 KB	
□ XML Topology		
□ Status		
Total		

Figure 19 Export Discovered SAN — Disk dialog box

2. Select an option from the Export To list:
   - **Disk**—Saves the exported files to the disk in `*Install_Home*\Client\Data\*sandate*\san*.zip.`
   - **EMail**—Mails the exported files as an e-mail attachment directly from the application.
3. Select the types of files that you want to export from the Files check boxes.

Depending on the export destination you selected in the previous step, some file types may not be available.

4. Performance data is an optional feature. If you purchased this option, you can select the switches for data export (Figure 20).



You have selected to export performance data. By default, HAFM 8 will include data for all switches. By limiting the number of switches, you can reduce the size of the export file.

Select Switches for Performance Data

	Nickname	IP Address	Node Name	File Size
☑		16.129.91.93	1000080088A0406F	2,574 ...
☑		16.129.91.83	1000080088A05456	1,295 ...
☑		16.129.91.115	1000080088A0B26D	5,406 ...
☑		16.129.91.111	1000080088A07C6A	654 KB
☑		16.129.91.116	100008008860308C	912 KB

Only include files of last

☑ Hour ☑ Day ☑ Week ☑ Month ☑ Year ☑ Max

Figure 20 Select Switches dialog box

NOTE: You can click **Select All** to include all switches or you can click **Unselect All** to remove all switches.

---

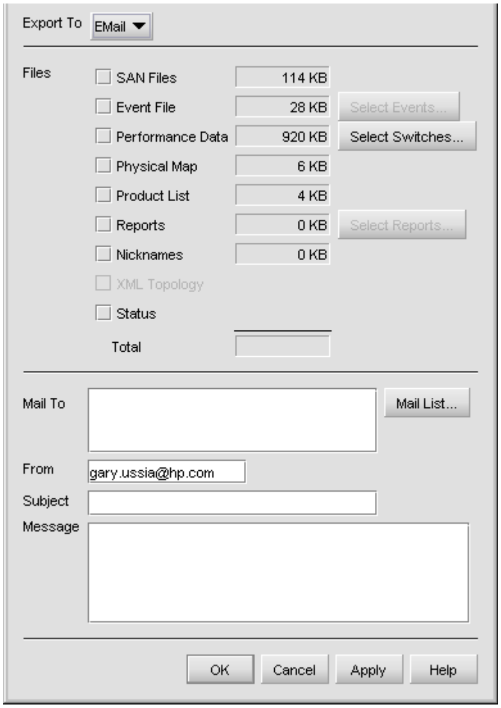
a. Select the check box for each switch that you want performance data for.
b. Select what you want from the **Only include performance files of last** check boxes.
c. Click **Apply to All** if you want the information selected in step 4b to apply to all switches.
d. Click **OK**.

NOTE: The Product List is exported in tab-delimited format. To view the Product List in table format, open it in Microsoft Excel.

---

5. If you are exporting to disk, proceed to step 8.

6. If you are exporting to e-mail, the email information is displayed (Figure 21).



Export To: EMail

Files

□ SAN Files	114 KB
□ Event File	28 KB
□ Performance Data	920 KB
□ Physical Map	6 KB
□ Product List	4 KB
□ Reports	0 KB
□ Nicknames	0 KB
□ XML Topology	
□ Status	
Total	

Mail To:

From: gary.ussia@hp.com

Subject:

Message:

Figure 21 Export Discovered SAN — Email dialog box

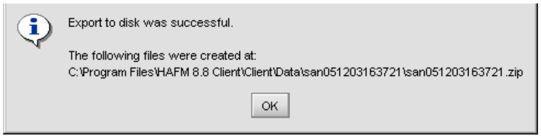
7. Enter information in the following boxes:
   - Mail To

NOTE: Click **Mail List** to display the Mail List dialog box.

   - From
   - Subject
   - Message

8. Click **OK**.

   A confirmation message is displayed (Figure 22).



Export to disk was successful.

The following files were created at:
C:\Program Files\HAFM 8.8 Client\Client\Data\san051203163721\san051203163721.zip

Figure 22 Export confirmation message

9. Make a note of the file location and name and click **OK**.

Importing data

You can import the following information to the application:

- **SAN File (zip)**—Imports an entire SAN in zip format.
- Nicknames—Imports the nicknames that were assigned to HP switches using the HAFM appliance and displays them on the Physical Map and Product List as product labels. Nicknames must have been defined in the Node List View of the HAFM appliance. Nicknames defined in the Configure Ports area will not be imported. The WWNs in the nicknames file are assumed to be port WWNs. If this file uses the node WWN, no import will take place. The nicknames file is located in `C:\EfcData\EmsData\efcHafmServices\WwnNicknames`.
- **Properties (csv)**—Imports properties of products and ports, including labels and IP addresses. The general format for this import is in comma-separated value (CSV) ASCII format. The first line defines the kind of import (Node or Port) and lists the properties and columns in the Product List. The first column must be either Node Name or Port Name. Subsequent columns contain property (column) names. These properties can be standard (for example, Label), or user-defined (for example, Cabinet Color). Non-editable properties will not be imported (for example, Port Count). Non-existent columns will be ignored. The format is space sensitive (only commas are used as separators), so trim leading or trailing spaces unless you want to import them as part of the data. To import port properties, use the Port Name column header. Port import will only allow the Label property to be set.
- **HBA Node Name**—Imports data to an HBA, use Node import but specify the HBA's port WWN in the Node Name column. This is necessary since the HBA's node WWN does not uniquely identify an HBA. Using the port WWN makes it possible to uniquely specify an HBA.
- **Server HBA Mappings (csv)**—Imports Server HBA Mappings into the existing Fabric Map. The general format for this import is in comma-separated value (CSV) ASCII format. The first row contains the header for the file, which does not effect the import process; however, text must be present. The first two boxes must be the World Wide Port Name (WWNN), then the Server Nickname. If either of these boxes is empty, the entry is null and is not imported. All additional boxes are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data.
- **Storage Port Mappings (csv)**—Imports Storage Port Mappings into the existing Fabric Map. The general format for this import is in comma-separated value (CSV) ASCII format. The first row contains the header for the file, which does not effect the import process; however, text must be present. The first two boxes must be the WWPN, then the Storage Device Nickname. If either of these boxes are empty, the entry is null and is not imported. All additional boxes are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data.

△ **CAUTION:** Importing files clears the Master Log of previous events.

To import files:

1. Select **SAN > Import**.

   The Import dialog box is displayed (Figure 23).

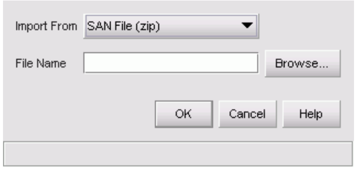


Figure 23 Import dialog box

2. Select the type of file you want to import from the Import From list.
3. Enter the path and file name in the File Name box.

NOTE: The default path is `Install_Home\ClientData\san<date>\san*.zip`. Importing the `rep*.zip` file causes errors.

4. Click **OK**.

   A confirmation message box is displayed.

   - If you selected SAN File, Nicknames, or Properties, continue with step 5.
   - If you selected Server HBA Mappings or Storage Port Mapping, go to step 6.
5. If you are sure you want to replace the data on the appliance, click **OK**.

   If you are importing a SAN file or a properties file, the client is logged out and the HAFM 8.8 Log In dialog box is displayed.
6. Log back in to the application.

NOTE: When discovery is on, the discovered SAN is replaced with the imported data. For information about discovery, see "Configuring discovery" on page 72.

Backing up and restoring data

You can protect your SAN data by backing up the data and then restoring it when necessary. The HAFM appliance provides a platform for the Enhanced Base package of the HAFM application. This provides more memory for future product enhancements.

Several types of appliance platforms can be available:

- The rack-mount appliance provides a platform for the Enhanced Base package of HAFM. This unit provides more memory for future product enhancements.
- Customer-supplied server.

The following data is backed up from the *Install_Home*`\Call_Home`, *Install_Home*`\Server` and *Install_Home*`\Client` directories:

- All log files
- Zoning library
- Call-home configuration (including phone numbers and dialing options)
- Configuration data
- Plans
- License information
- User launch scripts
- User-defined sounds
- All data exported through the Export option on the SAN menu

NOTE: Firmware files are *not* backed up.

Backing up data

If you keep a CD-RW disk in the CD recorder drive of the appliance, critical data from the HAFM application is automatically backed up to the CD-RW disk when the data directory contents change or when you restart the HAFM application.

Restoring data

Allow 45 minutes after making a configuration change before restoring data from the backup files. This ensures that all your changes are included in the backed up files. It is possible that, in a disaster recovery situation, configuration changes made less than 45 minutes before appliance loss could be missing from the backup.

To restore data to the appliance platforms, perform the following procedure:

1. Reinstall the application, if necessary.
2. Open the HAFM application on the HAFM appliance.
3. Select **SAN > Import**.

   The Import dialog box is displayed (Figure 23 on page 56).
4. Select **SAN File (zip)** from the Import From list.
5. Click **Browse**.

   The Browse dialog box is displayed.
6. Select the following file:

   `CD Drive\Backup\Server\Data\Backup\BkpPersisted.zip`
7. Click **Open**.
8. Click **OK**.

   A message box is displayed indicating that imported data replaces corresponding data on the appliance.
9. If you are sure you want to replace the data on the appliance, click **OK**.

   The client is logged out and the Login dialog box is displayed.

10. Log back into the application.
11. Stop the HAFM Services by selecting **Start > Programs > HP StorageWorks ha-fabric manager 8.8 > Stop Services**.

    A DOS window displays messages of services being shut down.
12. To restore data to the HAFM appliance, complete the following:
    a. Copy the three folders (Call Home, client, and server) from the CD-ROM drive (`X:\Backup\`*`directory`*) and paste them in `C:\Program Files\`*`Install_Home`*.

       A message is displayed asking if you want to overwrite the existing files.
    b. Click **Yes**.
13. Start HAFM Services by selecting **Start > Programs > HP StorageWorks ha-fabric manager 8.8 > Start Services**.
14. Ensure discovery is turned on by selecting **Discover > On**.

Customer-supplied server backup

There are three options for backing up with HAFM:

- Backing up to a read writable CD
- Backing up to a hard drive
- Backing up to a network drive

Backing up data

HAFM backs up data to two alternate folders. For example, if the backup directory location is `D:\Backup`, the backup service alternates between two backup directories, `D:\Backup` and `D:\BackupAlt`. The current backup is always `D:\Backup` and contains a complete backup of the system. The older backup is always `D:\BackupAlt`.

If a backup cycle fails, usually because the CDRW is full, there may be only one directory, `D:\Backup`. There can also be a `D:\BackupTemp` directory, which you should ignore as it can be incomplete.

Backing up to a CD-RW

To back up to a CD-RW, you must have CD writing software installed, and the disk must be formatted by the software so that it behaves like a drive.

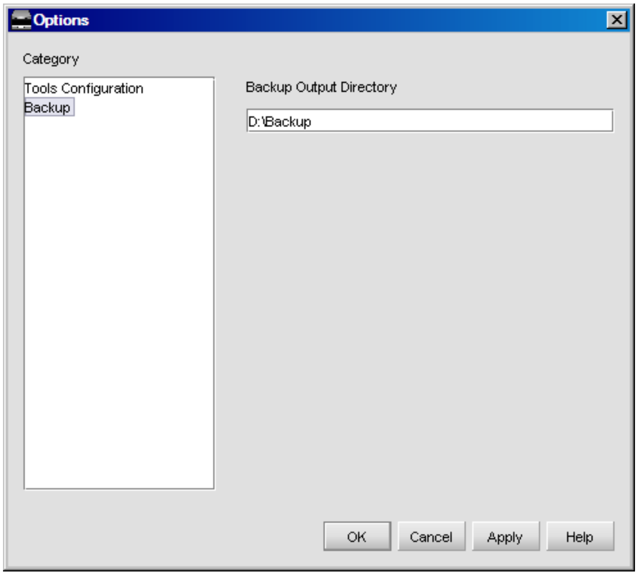
1. Select **SAN > Options**.

   The Options dialog box is displayed (Figure 24 on page 59).
2. Select **Backup** in the Category list.

   The currently defined directory is displayed in the Backup Output Directory box.
3. Click **Browse** and select the hard drive and directory to which you want to back up your data.

   The default directory is `D:\Backup`. It is assumed that the D: drive is a CD-RW drive.

Browse is only available on a local client, not a remote client.



Backup Output Directory

D:\Backup

Figure 24 Options dialog box

4. Click **Apply** or **OK**.

   For local clients, the application verifies that the device exists. If the device does not exist, an error message indicates that you have specified an invalid device.

5. Insert the formatted disk in the CD drive.

   Backups occur at 15-minute intervals.

NOTE: CDs have a limited life and may only last about a month. An error message is displayed if your HAFM appliance can no longer backup to the CD.

Backing up to a hard drive

1. Select **SAN > Options**.

   The Options dialog box is displayed.

2. Select **Backup** in the Category list.

   The currently defined directory is displayed in the Backup Output Directory box.

3. Click **Browse** and select the hard drive and directory to which you want to back up your data.

   The default directory is `D:\Backup`. It is assumed that the D: drive is a CD-RW drive.

   Browse is only available on a local client, not a remote client.

4. Click **Apply** or **OK**.

   For local clients, the application verifies that the device exists. If the device does not exist, an error message indicates that you have specified an invalid device.

   Backups occur at 15-minute intervals.

Backing up to a network drive.

To back up to a network drive, your workstation must be in the same domain and you must have rights for the network drive in order to copy files. The System Administrator can verify the user rights to the network drive. The network drive must be mounted on the appliance.

1. Select **Start > Settings > Control Panel > Administrative Tools > Services**.

   The Services dialog box is displayed.
2. Right-click **BK_MGR** and select **Properties**.

   The Properties dialog box is displayed.
3. Click **Log On**.
4. Click **This account** and enter the account name for the user who has rights to the network drive.
5. Enter a password in the **Password** and **Confirm password** boxes.
6. Click **OK** to apply changes and to close the BK_MGR Properties dialog box.
7. Click the close (X) icon on the Services dialog box.
8. Select **SAN > Options** on the HAFM appliance.

   The Options dialog box is displayed.
9. Select **Backup** in the Category list.

   The currently defined directory is displayed in the **Backup Output Directory** box.
10. Click **Browse** and select the mapped network drive and directory to which you want to back up your data.

    The default directory is `D:\Backup`. It is assumed that a D: is a CD-RW drive. **Browse** is only available on a local client, not a remote client.
11. Click **Apply** or **OK**.

    For local clients, the application verifies that the device exists. If the device does not exist, an error message is displayed indicating that you have specified an invalid device.

    If your are using a remote client, when you click **Apply** or **OK**, HAFM does not verify that the drive exists, it just saves the settings. Backups occur at 15-minute intervals.

Accessing to Eclipse management applications

This section describes how to configure HAFM to launch the following Eclipse SAN Router management applications:

- **SANvergence Manager**—Launch this application by right-clicking a SAN Router icon on the Physical Map and selecting **SANvergence Manager**.
- **SAN Router Element Manager**—Launch this application by right-clicking a SAN Router icon on the Physical Map and selecting **Element Manager**.

  To launch a SAN Router Element Manager when SANvergence Manager is operating:

  - Select the SAN Router in an expanded mSAN list in the left pane of the SANvergence Manager window, and then click the Element Manager icon at the top of the window.
  - Select the SAN Router in the SAN Routers table in the right pane of the SANvergence Manager window when an mSAN cloud is selected, and then click the Element Manager icon at the top of the window.

NOTE: You cannot launch SANvergence Manager or Element Manager by selecting the router proxy port icons (domain IDs 30 and 31). You must select the icon for the actual SAN Router.

Configuring access

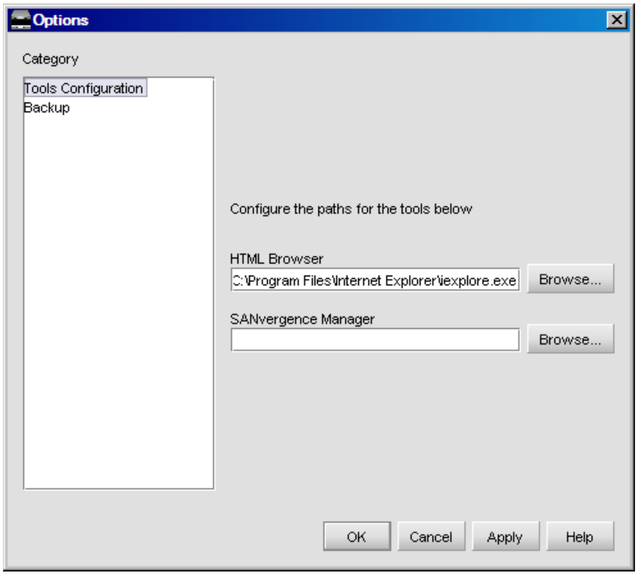
To configure HAFM to launch Eclipse SAN Router management applications:

1. Select **SAN > Options**.

   The Options dialog box is displayed (Figure 24 on page 59).

2. Select **Tools Configuration** in the Category list.

   The Options dialog box is displayed with the Tools Configuration options (Figure 25).



Options

Category

Tools Configuration
Backup

Configure the paths for the tools below

HTML Browser
C:\Program Files\Internet Explorer\iexplore.exe

SANvergence Manager

Figure 25 Options dialog box (Tools Configuration)

3. To configure the application to launch SAN Router Element Managers:

   a. Click **Browse** for the HTML Browser box.

   b. Browse to the install location of your web browser. For Internet Explorer, the default is `C:\Program Files\Internet Explorer`.

   c. Select the browser executable file in the **Locate the Browser** dialog box, and then click **Select File**.

   For Internet Explorer, select `iexplore.exe`.

4. To configure the application to launch SANvergence Manager:

   a. Click **Browse** for the SANvergence Manager box.

   b. Browse to the install location for SANvergence Manager. The default is `C:\Program Files\McDATA\SANvergence Manager xx`.

where xx is the current release number.

c. Select **SM.bat** file in the **Locate the Browser** dialog box, and then click **Select File**.

d. Click **OK**.

Configuring Call Home for remote dial-in

To run the Call Home service:

- For remote dial-in to work, RAS must be installed and configured on your appliance.
- The modem must be sent to auto answer.
- A new user, srvacc, must be configured with Administrator privileges.
- The PC must be configured for dial-in connections with the correct IP addresses.
- The srvacc user must be allowed to connect via dial-in.

Miscellaneous

If a web server is running on the PC, such as IIS, then the default embedded http server port needs to be configured for another port by adding the following property to the `C:\Program Files\HAFM 8.5\resources\server\Config.properties` file:

```
Smp.server.httpserverport=<port number>
```

Multiple network interface cards

A second Ethernet NIC may be desirable in the PC to isolate the switches in your SAN from the public network. If there are any connection issues with the dual NICs, a configuration file (`C:\Program Files\HAFM 8.5\resources\Server\config.properties`) can be modified to force the appliance to look at a specific IP address.

1. Add the following parameter to the file:

   ```
   ServerRmIpAddress=xxx.xxx.xxx.xxx
   ```

   where `xxx.xxx.xxx.xxx` is the IP address of the NIC card that you want the client connections to come in on.

2. Follow the instructions provided by the InstallShield wizard.

3 Managing the HAFM application

This chapter provides instructions for managing and customizing the application.

Accessing HAFM

You can access HAFM in one of two ways:

- Log in from a browser-capable PC connected through an Ethernet LAN segment.
- Log in remotely with an HAFM client application.

See "Accessing HAFM" on page 63 for login instructions.

Adding and removing a network address

When you log in to the appliance, the network address that you enter is added to the network address list on the HAFM 8.8 Log In dialog box.

△ **CAUTION:** This procedure deletes the appliance from the network address list without prompting you for a confirmation.

To remove a network address from the list in the HAFM 8.8 Log In dialog box:

1. Turn on the HAFM appliance, or if the appliance is already turned on, double-click the **HAFM** icon on the desktop.

   The HAFM 8.8 Log In dialog box is displayed (Figure 3 on page 31).
2. Select the appliance you want to remove from the Network Address list.

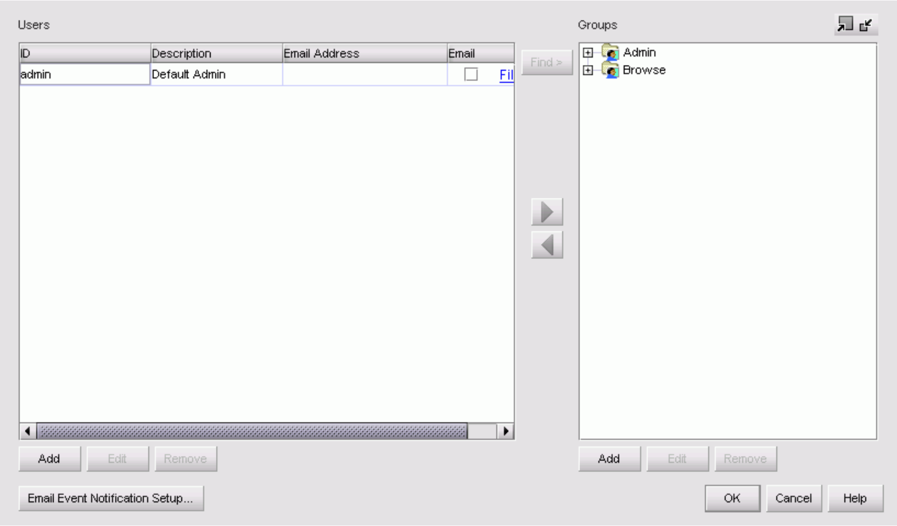
   The selected appliance's IP address is displayed in the Network Address box.
3. Click **Delete**.

Managing users

To grant access to the HAFM application, the administrator can assign user names, passwords, and access rights. The administrator can configure up to 16 users in an HAFM application; but no more than 9 users (8 remote and 1 local user) can simultaneously access the HAFM appliance. Access rights are defined by the user groups as described in "Managing user groups" on page 68.

Viewing the list of users

Select **SAN > Users** to view a list of users, their event notification settings, their e-mail addresses, and a list of user groups to which they belong in the Server Users dialog box (Figure 26).



Users

ID	Description	Email Address	Email
admin	Default Admin		□ Fil

Groups

- ⊞ Admin
- ⊞ Browse

Figure 26 Server Users dialog box

Adding a user account

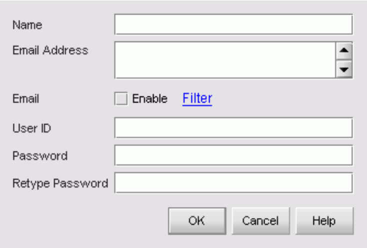
To add a user account:

1. Select **SAN > Users**.

   The Server Users dialog box is displayed (Figure 26).

2. Click **Add**.

   The Add User dialog box is displayed (Figure 27).



Name

Email Address

Email □ Enable Filter

User ID

Password

Retype Password

Figure 27 Add/Edit User dialog box

3. Enter the user information in the following boxes:
    - Name
    - Email Address, separating multiple addresses with a semicolon
    - User ID
    - Password
    - Retype Password
4. Select **Enable** to enable e-mail notification for the user.

   A message can display stating that you must enable event notification for the SAN. Click **Yes**.
5. Click the **Filter** link to specify the event types for which to send e-mail notifications to this user. See "Filtering event notifications for a user" on page 66 for details.
6. Click **OK**.

   The new user is displayed in the Server Users dialog box.
7. Click **OK**.

Changing a user account

To modify a user account:

1. Select **SAN > Users**.

   The Server Users dialog box is displayed (Figure 26 on page 64).
2. Select the user whose information you want to edit.
3. Click **Edit**.

   The Edit User dialog box is displayed (Figure 27 on page 64).
4. Edit the information as necessary.
5. Click **OK**.

   The edited information is displayed in the Users dialog box.
6. Click **OK**.

Removing a user account

△ **CAUTION:** This procedure removes the user's account without prompting you for confirmation.

To remove a user account:

1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).
2. Select the user account you want to remove.
3. Click **Remove**.
4. Click **OK**.

NOTE: If the user is logged in when you remove the account, the account is not affected until the user logs out and attempts to log in again.

Filtering event notifications for a user

The application provides notification of many different types of SAN events. If a user needs to know only about certain events, you can specify which event notifications are sent to that user.

To filter event notification:

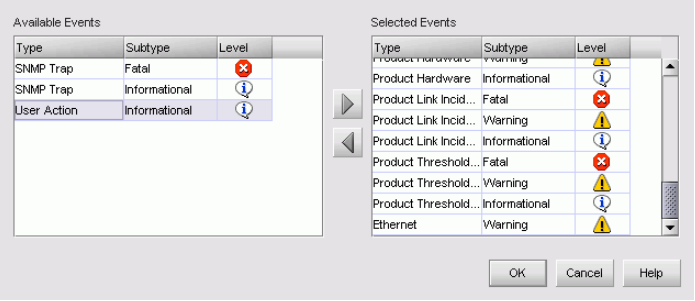
1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).

2. Click the **Filter** link in the **Email** column associated with the user for whom you want to filter events.

   The Filter dialog box is displayed (Figure 28).

   The Selected Events table includes the events of which this user is notified. The Available Events table includes all other events.



Available Events

Type	Subtype	Level
SNMP Trap	Fatal	✖
SNMP Trap	Informational	ⓘ
User Action	Informational	ⓘ

Selected Events

Type	Subtype	Level
Product Hardware	Warning	⚠
Product Hardware	Informational	ⓘ
Product Link Incid...	Fatal	✖
Product Link Incid...	Warning	⚠
Product Link Incid...	Informational	ⓘ
Product Threshold...	Fatal	✖
Product Threshold...	Warning	⚠
Product Threshold...	Informational	ⓘ
Ethernet	Warning	⚠

Figure 28 Filter dialog box

3. Move events between the tables by selecting the event and clicking the appropriate arrow button.
4. Click **OK**.

   The Users dialog box opens.

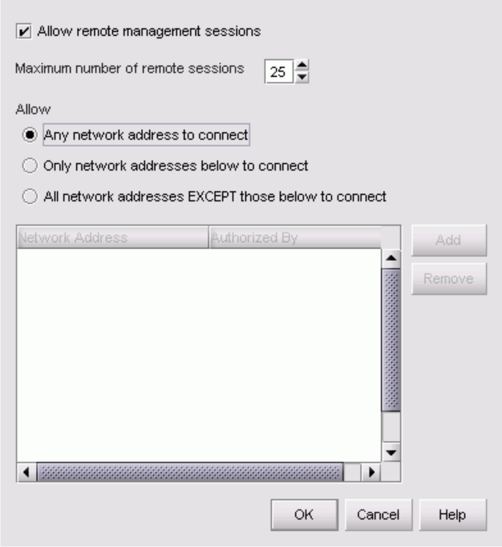
5. Turn on event notification for the user by selecting the **Filter** check box.
6. Click **OK**.

Configuring remote management access

To specify the network addresses that can access the appliance:

1. Select **SAN > Remote Access**.

   The Remote Access dialog box is displayed (Figure 29).



☑ Allow remote management sessions

Maximum number of remote sessions 25

Allow

● Any network address to connect

○ Only network addresses below to connect

○ All network addresses EXCEPT those below to connect

Figure 29 Remote Access dialog box

2. Select **Allow remote management sessions** to allow others to access the appliance remotely.
3. Enter the maximum number of remote sessions you want to allow.
4. Select whether to allow all or some network addresses to connect.
5. If you select **Only network addresses below to connect** or **All network addresses EXCEPT those below to connect**, enter the appropriate addresses in the **Network Address** box.
   - To add an address, click **Add**, enter a network address, and then click **OK**.
   - To remove an address, highlight the address in the table and click **Remove**.
6. Click **OK**.

Disconnecting a user

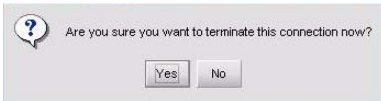
To disconnect a use:

1. Select **SAN > Active Sessions**.

   The Active Sessions dialog box is displayed.

2. Select the user that you want to disconnect and click **Disconnect User**.

   A message box is displayed (Figure 30).



Are you sure you want to terminate this connection now?

Figure 30 Disconnect User message box

3. Click **Yes**.
   - The user is disconnected.
   - The appliance immediately shuts down the appliance-client connection.
   - The status bar on the client window shows a message stating that the appliance connection was lost.
   - All products and connections on the Physical Map stay in the condition they were in when the session ended; they do not turn grey.
   - The client window shows a message stating that a user disconnected the client from the appliance.

NOTE: To prevent this user from reconnecting, remove the user account. See "Removing a user account" on page 65.

Managing user groups

User groups are a security feature that define allowable access to information and system features. System Administrators determine each user's needs and assign an appropriate user group. This section provides an overview of user groups and their access levels, and describes how to set up a user group.

Understanding user groups and access levels

Table 13 lists the four preconfigured user groups available with the application. A System Administrator can create additional user groups to provide users access to specific features and views. Users can be assigned the following types of access to features:

- **Read/write access**—The ability to view and edit information.
- **Read-only access**—The ability to view information; edit and configuration capabilities are disabled.
- **No access**—Access to information is denied.

Table 13 User groups and access levels

User group	Description
System Administrator	Read/write access for all features; all functions are enabled and allowed
Maintenance	Read/write access for Call Home event notification, device maintenance, and e-mail event notification setup Read-only access for all other features
Operator	Read/write access for device operation Read-only access for all other features
Product Administrator	Read/write access for device administration Read-only access for all other features

Creating a user group

To create a user group and specify access to certain features and views in the application:

1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).

2. Click **Add** below the Groups table.

   The Group dialog box is displayed (Figure 31).

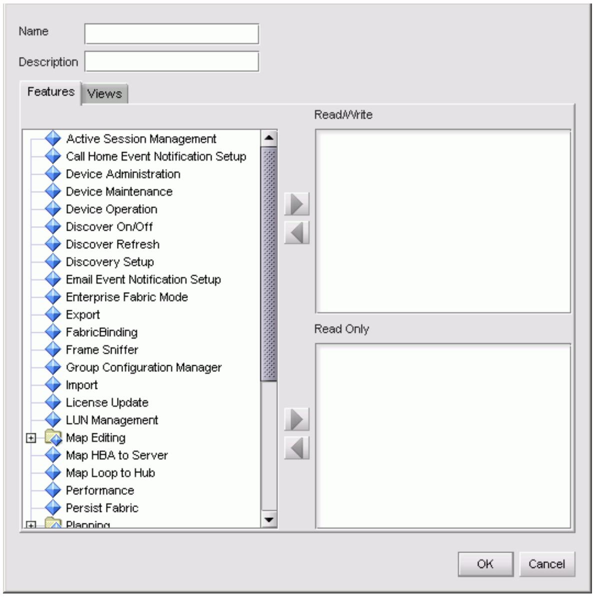


Figure 31 Group dialog box

3. Enter information for the new user group in the following boxes:
   - Name
   - Description
4. If you want to assign permission to use only certain views, proceed to step 9.

   If you want to assign permission to use certain features, proceed to step 5.
5. Select the features for which you want to provide read/write access in the features list.
6. Click ▷ next to the Read/Write list.

   The features are moved to the Read/Write list.
7. Select the features for which you want to provide read-only access in the features list.
8. Click ▷ next to the Read Only list.

   The features are moved to the Read Only list.
9. Click the **Views** tab.
10. Select the views you want the user group to be permitted to access in the Available Views list.
11. Click ▷ to move the selections to the Selected Views list.
12. Click **OK**.

    The new group is displayed in the Groups list of the Users dialog box. To add users to this group, follow the instructions in "Assigning users to groups" on page 71.
13. Click **OK**.

Changing a user group

An administrator can change a user group's access to certain features and views. This provides added security for your SAN as well as your management application.

To change a user group:

1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).
2. Select the user group to be changed.
3. Click **Edit** below the Groups list.

   The Group dialog box is displayed (Figure 31).
4. Select the features that you want to change, and click the appropriate arrow to move them to another list.
5. Click **OK**.

   The Users dialog box is displayed.
6. Click **OK** to accept the changes.

Removing user groups

△ **CAUTION:** This procedure removes the user group without prompting you for a confirmation.

An administrator can remove a user group, regardless of whether any users are assigned to the group.

To remove a user group:

1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).
2. Select the group you want to remove from the Groups list.
3. Click **Remove** located below the Groups list.
4. Click **OK**.

Assigning users to groups

An administrator assigns users to groups to provide access to features and topology views. If an administrator assigns one user to multiple groups, the user has access rights specified in all the groups.

NOTE: If a user is logged in when you reassign the group, the account is not affected until the user logs out and logs in again.

To assign a user to an existing group:

1. Select **SAN > Users**.

   The Users dialog box is displayed (Figure 26 on page 64).
2. Select a user in the Users list.
3. Select the groups to which you want to assign the user in the Groups list.
4. Click ▷.

   The user is assigned to the selected groups.
5. Click **OK**.

Determining user groups

An administrator can determine the groups to which a user belongs through the HAFM Users dialog box.

To determine user groups:

1. Select **SAN > Users**.

   The HAFM Users dialog box is displayed (Figure 26 on page 64).
2. Select a user in the Users list.
3. Click **Find**.

   The groups to which the user belongs are highlighted in the Groups list.
4. Click **OK**.

Discovering a SAN

The application discovers products, fabrics, and connections in a SAN. Through discovery, you can manage and monitor your SAN in real time, ensuring that any issues are resolved immediately. This section provides instructions for configuring the discovery feature.

Understanding how discovery works

Discovery is the process by which the application contacts the devices in the SAN. The application illustrates each product and its connections on the Physical Map. After you log in and configure and turn on discovery, the application discovers products connected to the SAN.

When performing out-of-band discovery, the application connects to the switches through the IP network, and product information is copied from the SNS database on the switch to the appliance.

Only fabrics that have HP switches as the principal switch are displayed. If a HP switch is being directly managed, but exists in a fabric where the principal switch is a third-party device, another appliance is not allowed to connect to and manage that device.

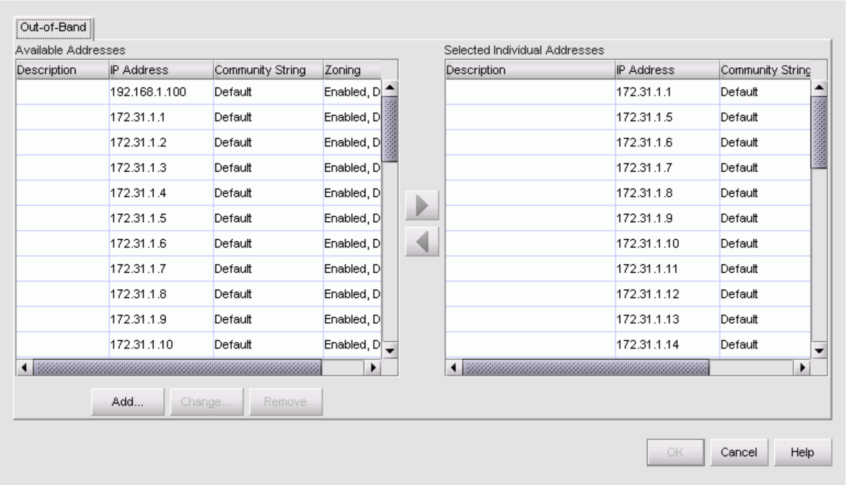
NOTE: Ensure that your SNMP communication parameters are set correctly in order to discover switches. Otherwise, the discovery can fail.

Configuring discovery

To define the devices you want discovery to find:

1. Select **Discover > Setup**.

   The Discover Setup dialog box is displayed (Figure 32).



Available Addresses

Description	IP Address	Community String	Zoning
	192.168.1.100	Default	Enabled, D
	172.31.1.1	Default	Enabled, D
	172.31.1.2	Default	Enabled, D
	172.31.1.3	Default	Enabled, D
	172.31.1.4	Default	Enabled, D
	172.31.1.5	Default	Enabled, D
	172.31.1.6	Default	Enabled, D
	172.31.1.7	Default	Enabled, D
	172.31.1.8	Default	Enabled, D
	172.31.1.9	Default	Enabled, D
	172.31.1.10	Default	Enabled, D

Selected Individual Addresses

Description	IP Address	Community String
	172.31.1.1	Default
	172.31.1.5	Default
	172.31.1.6	Default
	172.31.1.7	Default
	172.31.1.8	Default
	172.31.1.9	Default
	172.31.1.10	Default
	172.31.1.11	Default
	172.31.1.12	Default
	172.31.1.13	Default
	172.31.1.14	Default

Figure 32 Discover Setup dialog box

NOTE: To discover all SAN products, you must specify each product's IP address in the Discover Setup dialog box (Out-of-Band tab). If you do not configure the application to discover the devices directly, the connections and attached devices may not be correct on the window.

2. Select IP addresses from the Available Addresses list and add them to the Selected Individual Addresses list by clicking the right arrow (▶) button.
3. Click **OK**.
4. Click **Add** to specify the IP addresses you want to discover through out-of-band discovery.

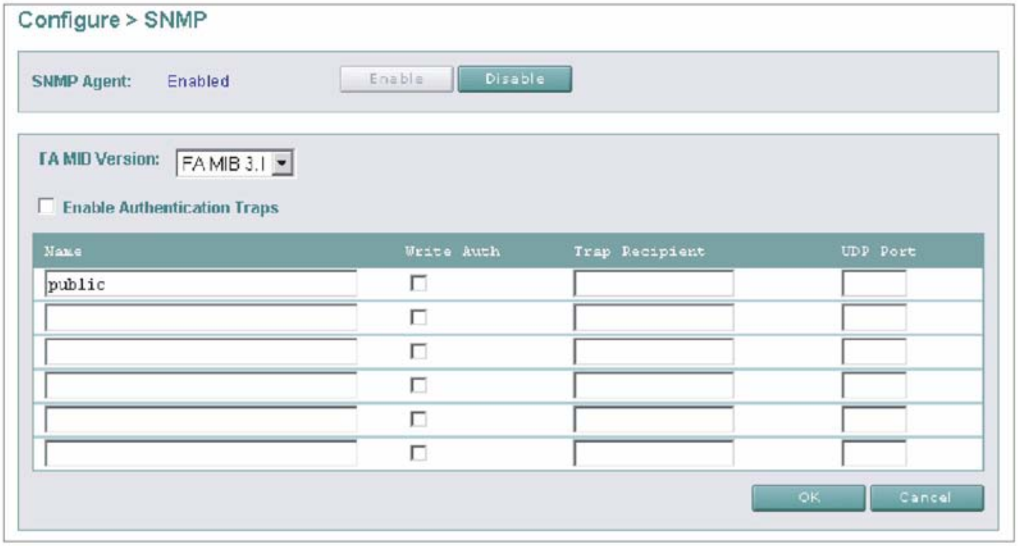
   You can add, change, and remove IP addresses as necessary. See "Configuring IP addresses and community strings" on page 76 for instructions.
5. Select the entries from the Selected Individual Addresses list that you do not want to discover now, and move them back to the Available Addresses list by clicking the corresponding left arrow button.
6. Click **OK**.
7. Turn discovery on or off by selecting **Discover > On** or **Discover > Off**.

Troubleshooting discovery

If you encounter discovery problems, use the following procedure to ensure that discovery was set up correctly:

1. Verify IP connectivity by pinging the switch.
   - **a.** Display the command prompt.
   - **b.** From the server, type `ping` *switch IP address*.
2. Verify the SNMP settings.
   - **a.** Launch HAFM Basic interface by opening a web browser and entering the IP address of the product as the Internet URL.
     For example, http://10.1.1.11.
   - **b.** Log in and click **OK**.
   - **c.** Select **Configure > SNMP**.

The SNMP view is displayed (Figure 33).



Configure > SNMP

SNMP Agent: Enabled

FA MIB Version: FA MIB 3.1

□ Enable Authentication Traps

Name	Write Auth	Trap Recipient	UDP Port
public	□		
	□		
	□		
	□		
	□		
	□		

Figure 33 SNMP view

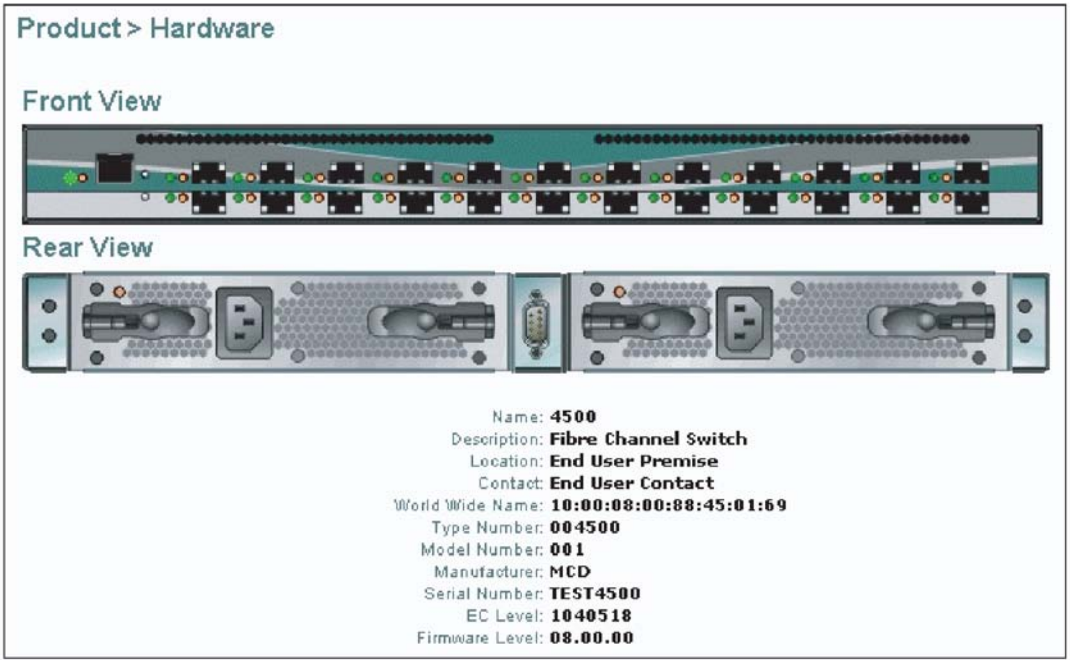
d. Verify that the **SNMP Agent** is enabled. If not, then click **Enable**.

e. Verify that the Name box displays `public` or matches the HAFM appliance configuration.

3. Verify the product data.

   a. Select **Product > Hardware**.

The Hardware view is displayed (Figure 34).



Product > Hardware

Front View

Rear View

Name: 4500
Description: Fibre Channel Switch
Location: End User Premise
Contact: End User Contact
World Wide Name: 10:00:08:00:88:45:01:69
Type Number: 004500
Model Number: 001
Manufacturer: MCD
Serial Number: TEST4500
EC Level: 1040518
Firmware Level: 08.00.00

Figure 34 Hardware view

b. Verify that the WWN has the correct syntax (`xx:xx:xx:xx:xx:xx:xx:xx`).

c. Verify that the Type Number is one of the following:

003016
003032
003216
003232
004300
004500
005000
006064
006140

4. Verify SNMP connectivity.

a. Use a third-party MIB browser to verify the SNMP connection.

b. Change the SNMP default timeout:

- Stop the server.
- Increase the default SNMP settings. If the device is running heavy traffic or is known to have slow SNMP response time, moderately increase the SNMP timeout (default timeout is one second) and retry count (default count is one retry).

- These two values are controlled by two VMParameters residing in the `bin\HAFMService.ini` file when the application is running as a Windows service: smp.snmp.timeout and smp.snmp.retries. For example, specifying "`-Dsmp.snmp.timeout=5`" and "`-Dsmp.snmp.retries=1`" instructs the server to use five seconds as the SNMP timeout and one retry as the retry count.

NOTE: The higher the values, the longer discovery will spend waiting for a SNMP response. This translates to slower system performance.

- Restart the server.

Configuring IP addresses and community strings

You can alter the database of selected IP addresses, SNMP community strings, Product type, and Access that the application uses to perform discovery, communication functions, and password authentication.

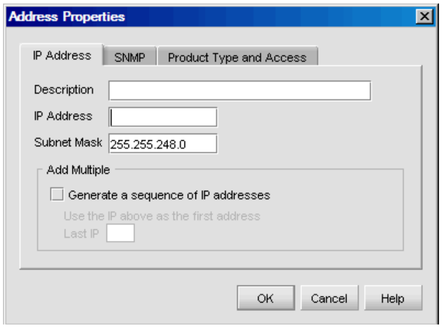
Adding an IP address

To add IP addresses and subnets through which the SAN can be discovered:

1. Select **Discover > Setup**.

   The Discover Setup dialog box is displayed (Figure 32).
2. Click **Add**.

   The Address Properties dialog box is displayed (Figure 35).
3. Click the IP Address tab.



Subnet Mask 255.255.248.0

□ Generate a sequence of IP addresses

Use the IP above as the first address

Last IP

Figure 35 Address Properties dialog box (IP Address tab)

4. Enter the appropriate information for the product in the following boxes:
   - Description
   - IP Address
   - Subnet Mask
5. To generate a sequence of IP addresses:
   - Select the **Generate a sequence of IP addresses** check box.
   - Enter the last IP address in the Last IP box.

NOTE: All IP addresses in a sequence must be on the same subnet and have the same first three octets.

6. Click **OK**.

Changing an IP address

To edit IP addresses or associated subnets that are listed on the Discover Setup dialog box:

1. Select **Discover > Setup**.
   The Discover Setup dialog box is displayed (Figure 32 on page 72).
2. Select the IP address you want to change from the Available Addresses list.
3. Click **Edit**.
   The Address Properties dialog box is displayed (Figure 35 on page 76).
4. Edit the information as necessary.
5. Click **OK**.
6. Click **OK**.

Removing an IP address

△ **CAUTION:** This procedure removes the IP addresses without prompting you for a confirmation.

To remove IP addresses from the Discover Setup dialog box:

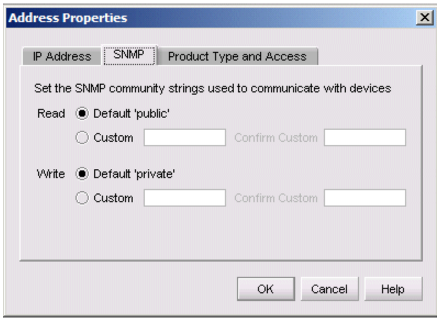
1. Select **Discover > Setup**.
   The Discover Setup dialog box is displayed (Figure 32 on page 72).
2. Select the IP address that you want to remove from the Available Addresses list.
3. Click **Remove**.
4. Click **OK**.

Configuring a community string

The community string defines read/write accessibility to devices. By default, the public community has read-only privileges, and the private community has read/write privileges. However, you can customize the community string. To specify community strings used to communicate with products, perform the following procedure:

1. Select **Discover > Setup**.
   The Discover Setup dialog box is displayed (Figure 32 on page 72).
2. Select the IP address that you want to change from the Available Addresses list.
3. Click **Add**.
   The Address Properties dialog box is displayed (Figure 35 on page 76).
4. Click the SNMP tab.

The SNMP tab is displayed (Figure 36).



Set the SNMP community strings used to communicate with devices

Read ● Default 'public'
○ Custom Confirm Custom

Write ● Default 'private'
○ Custom Confirm Custom

Figure 36 Address Properties dialog box (SNMP tab)

5. Select a Read option.
   - Select **Default 'public'** to select the default string.
   - Select **Custom** to specify a custom string.
6. Select a Write option.
   - Select **Default 'private'** to select the default string.
   - Select **Custom** to specify a custom string.
7. If you selected **Custom** in step 5 or step 6, continue to step 8. Otherwise, proceed to step 10.
8. Enter the custom string in the Custom box.
9. Enter the string again in the Confirm Custom box.
10. Click **OK**.
11. Click **OK** to close the Discover Setup dialog box.

Reverting to a default community string

To set the community string with default values:

1. Select **Discover > Setup.**

   The Discover Setup dialog box is displayed (Figure 32 on page 72).
2. Select an IP address from the Available Addresses list.
3. Click **Add**.

   The Available Addresses dialog box is displayed (Figure 35 on page 76).
4. Click the SNMP tab.

   The SNMP tab is displayed (Figure 36 on page 78).
5. Select **Default 'public'** and **Default 'private'**.
6. Click **OK**.

Configuring the product type and access

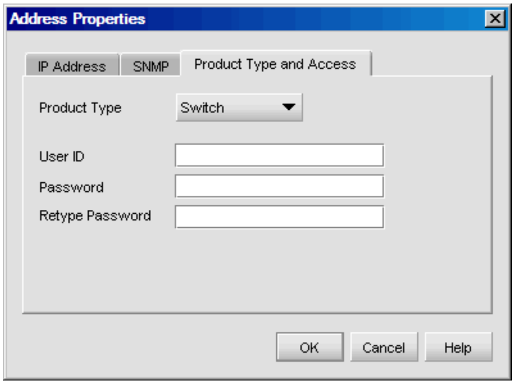
To specify the product type and set a user name and password for the address:

NOTE: The Product Type and Access tab may not be available in all situations.

1. Select **Discover > Setup**.

   The Discover Setup dialog box is displayed (Figure 32 on page 72).
2. Click **Add**.

   The Address Properties dialog box is displayed (Figure 35 on page 76).
3. Click the Product Type and Access tab. The Product Type and Access tab is displayed (Figure 37).


Address Properties

IP Address | SNMP | Product Type and Access

Product Type: Switch

User ID

Password

Retype Password

Figure 37 Address Properties dialog box (Product Type and Access tab)

4. Select the type of device from the Product Type list.
   - If you select `CIM/WBEM Services` from the Product Type list, enter a name in the Name Space box then go to step 14.
   - If you select `Clariion` from the Product Type list, go to step 16.
   - If you select `HDS` from the Product Type list, go to step 14.
   - If you select `HP XP Storage` from the Product Type list, go to step 14.
   - If you select `IBM ESS Storage` from the Product Type list, go to step 14.
   - 1If you select `NetApp` from the Product Type list, do the following:
     - Select the product protocol from the Protocol list.
     - Enter the product DFM port number in the DFM Port box.
     - Go to step 14.
   - If you select `<not specified>` from the Product Type list, go to step 16.
   - If you select `Switch` from the Product Type list, go to step 14.
   - If you select `Symmetrix` from the Product Type list, go to step 16.
5. Enter a user ID in the User ID box.
6. Enter the password in the Password and Retype Password boxes.
7. Click **OK**.

Turning discovery on and off

To turn discovery on or off, select **Discover > On** or **Discover > Off**.

Determining the operational status

NOTE: The Product List panel can be hidden by default. To view the Product List, select **View > Product List** or press **F9**.

You can determine a product's operational status by looking at the icons on the Physical Map or the Product List. Table 14 lists icons and operational statuses.

Table 14 Operational status

Icon	Operational status
No icon	Operational
⚠	Degraded
♦	Failed
❗	Unknown/link down

To see a list of all products requiring attention, click the Attention Indicator icon (⚠) on the Status bar at the bottom of the main window. The Service Request dialog box displays the names and IP addresses of devices needing attention. Click a product name hyperlink to jump to the product on the Physical Map. The list will update dynamically.

Determining the Discovery State

NOTE: The Product List panel can be hidden by default. To view all panels, select **View > All Panels** or press **F12**.

You can determine the discovery status of products by looking at the Status column in the Product List. Additionally, the operational status called Unknown is equivalent to the discovery state Offline. The operational statuses Operational, Degraded, and Failed are equivalent to the discovery state Online.

Configuring the SNMP agent

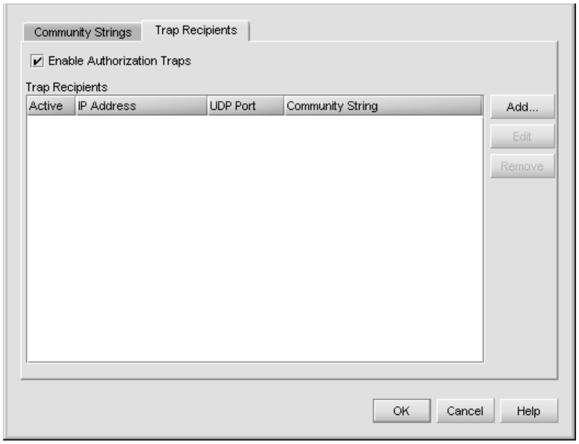
This section provides information to help you use the SNMP agent module.

Setting up the SNMP agent

The SNMP agent module implements the objects defined in the Fibre Channel Management (FCMGMT) Management Information Base (MIB) 3.1 and a small number of objects defined in MIB II. Through implementation of these MIB objects, the agent translates information stored on the appliance into a form usable by SNMP management stations.

You can configure network addresses and community names for up to 12 SNMP trap recipients. SNMP sends messages for specific events that occur on the appliance to trap recipients.

Figure 38 shows the dialog box used to configure the SNMP agent.



☑ Enable Authorization Traps

Figure 38 SNMP Agent Setup dialog box

Turning the SNMP agent on or off

To turn the SNMP agent on or off, select **Monitor > SNMP Agent > On | Off**.

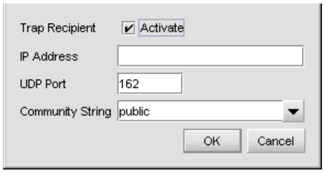
Configuring trap recipients

To configure the SNMP agent that runs on the appliance and implements the Fibre Alliance MIB:

1. Select **Monitor > SNMP Agent > Setup**.

   The SNMP Agent Setup dialog box is displayed (Figure 38).
2. Click the **Trap Recipients** tab.
3. Select **Enable Authorization Traps** if you want to enable messages to be sent when unauthorized management stations try to access SNMP information through the appliance.
4. Click **Add**.

The Add Trap Recipient dialog box is displayed (Figure 39).



Trap Recipient ☑ Activate

IP Address

UDP Port 162

Community String public

Figure 39 Add Trap Recipient dialog box

5. If you want this trap recipient to be active, select the **Activate** check box.
6. Enter the IP address or DNS host name of the trap recipient in the IP Address box.

   This name must be 64 characters or fewer.
7. Enter the User Datagram Protocol (UDP) port number in the Port box. This overrides the default UDP port number for a trap recipient with any legal, decimal UDP number.
8. Select a community string from the Community String list.
9. Click **OK**.

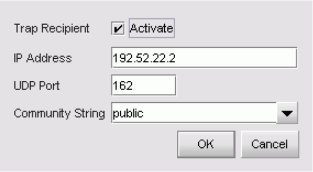
Editing trap recipients

To edit an existing trap recipient:

1. Select **Monitor > SNMP Agent > Setup**.

   The SNMP Agent Setup dialog box is displayed (Figure 38 on page 81).
2. Click the **Trap Recipients** tab.
3. Select the IP address of the trap recipient that you want to edit.
4. Click **Edit**.

   The Edit Trap Recipient dialog box is displayed (Figure 40).



Trap Recipient ☑ Activate

IP Address 192.52.22.2

UDP Port 162

Community String public

Figure 40 Edit Trap Recipient dialog box

5. Edit the information as necessary.
6. Click **OK**.

Removing trap recipients

△ **CAUTION:** This procedure removes trap recipients without prompting you for confirmation.

To remove an existing trap recipient from the list:

1. Select **Monitor > SNMP Agent > Setup**.

   The SNMP Agent Setup dialog box is displayed (Figure 38 on page 81).
2. Click the **Trap Recipients** tab.
3. Highlight the trap recipient that you want to remove.
4. Click **Remove**.
5. Click **OK**.

Customizing the main window

You can customize the main window by adjusting the level of detail displayed on the Physical Map or Product List columns. This helps to simplify management of large SANs. This section provides instructions for customizing the topology layout and creating user-defined views of the SAN.

You can create views that show only certain fabrics. If you discover or import a SAN with more than 2000 devices, the devices display on the Product List, but do not display on the Physical Map. Instead, the topology area shows a message stating that the topology cannot be displayed. You can create a new view to filter the number of devices being discovered.

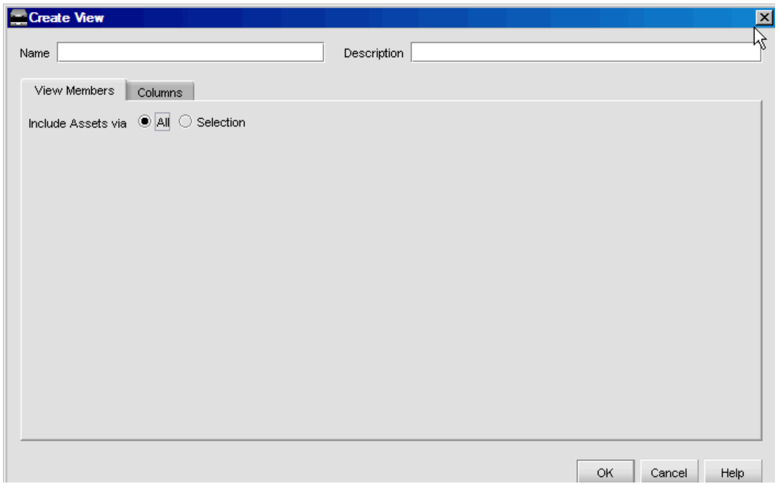
Creating a customized view

To customize the main window:

NOTE: Customized view settings reside on the appliance. All users who log on to the same appliance can select that view.

1. Do one of the following to open the Create View dialog box:
   - Select **View > Create View**.
   - Click the **View** tab and select **Create View**.

The Create View dialog box with the View Members tab is displayed (Figure 41).



Include Assets via ● All ○ Selection

Figure 41 Create View dialog box (View Members tab)

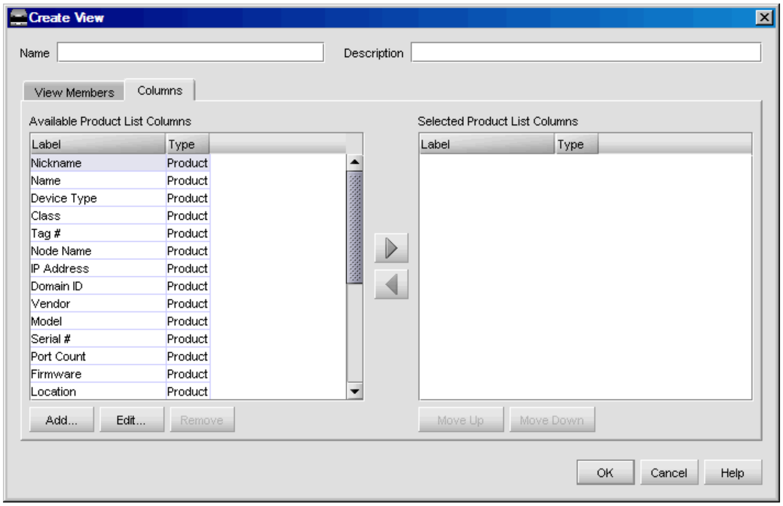
2. Enter information in the following boxes:
   - Name
   - Description
3. If you want to filter the fabrics that display on the Physical Map, continue to step 4; otherwise proceed to step 7.
4. Select Selection for the **Include Assets via** option.
5. Select the fabrics you want to include from the Available Fabrics list.

NOTE: **Other** in the Available Fabrics or Selected Fabrics lists refers to all isolated devices and connected sets. You see all newly discovered devices in the category even if the devices were not originally part of the view.

---

6. Click ▷ to move your selections to the Selected Fabrics list.
7. If you want to show or hide Product List columns, continue to step 8; otherwise, proceed to step 12.
8. Click the Columns tab.

The Create View dialog box with the Columns tab is displayed (Figure 42).



Available Product List Columns

Label	Type
Nickname	Product
Name	Product
Device Type	Product
Class	Product
Tag #	Product
Node Name	Product
IP Address	Product
Domain ID	Product
Vendor	Product
Model	Product
Serial #	Product
Port Count	Product
Firmware	Product
Location	Product

Selected Product List Columns

Label	Type

Figure 42 Create View dialog box (Columns tab)

9. Select the columns you want to see in the Product List from the Available Product List Columns list.
10. Click ▷ to move your selections to the Selected Product List Columns list.
11. To add, edit, or remove columns, see "Customizing the Product List" on page 86.
12. Click **OK**.

    The new view is displayed.

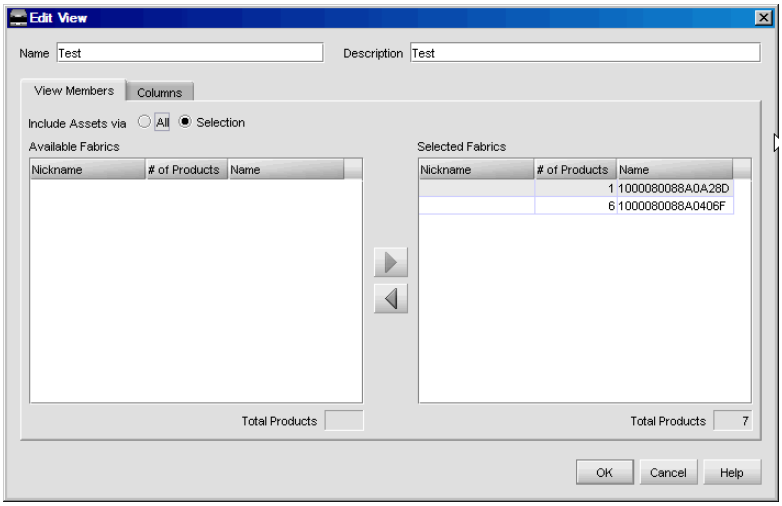
NOTE: If you select a customized view, any newly discovered devices are displayed.

Editing a customized view

To edit a customized view:

1. Select **View > Edit View**.

   The Edit View dialog box is displayed (Figure 43).
2. Select the view you want to edit.



Name: Test

Description: Test

Include Assets via ○ All ● Selection

Available Fabrics

Nickname	# of Products	Name

Total Products

Selected Fabrics

Nickname	# of Products	Name
	1	1000080088A0A28D
	6	1000080088A0406F

Total Products 7

Figure 43 Edit View dialog box

3. Edit the information as necessary.
4. Click **OK**.

Deleting a customized view

To delete a customized view:

1. Select **View > Delete View**.
2. Select the view you want to delete.
3. Click **OK**.

Selecting a customized view

To select a customized view, click the **View** tab and select the view name from the list.

Customizing the Product List

You can customize the Product List by creating views that display certain fabrics or certain levels of detail on the Product List.

Adding a column to the Product List

You can define new Product List columns. This enables you to further customize the Product List to display pertinent device and port information.

To add a column to a new or existing view:

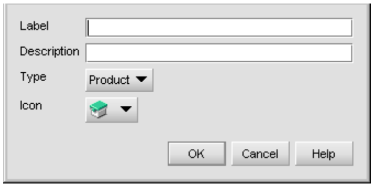
1. Perform one of the following to select a new or existing view:
   - Select **View > Create View**.

     The Create View dialog box is displayed (Figure 41 on page 84).
   - Select **View > Edit View** and select the view you want to edit.

     The Edit View dialog box is displayed (Figure 43 on page 86).
2. Click the **Columns** tab.

   The Create View dialog box with the Columns tab is displayed (Figure 42 on page 85).
3. Click **Add**.

   The Create Column dialog box is displayed (Figure 44).



Type Product

Figure 44 Create Column dialog box

4. Enter information for the new column in the following boxes:
   - Label
   - Description
5. Select whether the column shows information about products or ports from the Type list.
6. Select an icon to display in the column from the Icon list.
7. Click **OK**.
8. Select a column from the Available Product List Columns list and click ▷ to display the new column in the Product List.

   The column name moves to the Selected Product List Columns list.
9. Click **OK**.

   The new column is displayed in the Product List.

Changing a column on the Product List

To edit labels, definitions, information, and icons of existing Product List columns:

1. Select **View > Edit View**.
2. Select the view you want to edit.

   The Edit View dialog box is displayed (Figure 43 on page 86).
3. Click the **Columns** tab.

   The Create View dialog box is displayed (Figure 42 on page 85).
4. Click **Change**.

The Edit Column dialog box is displayed (Figure 45).

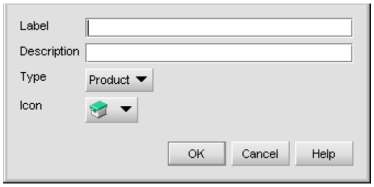


Figure 45 Edit Column dialog box

5. Edit the column properties as necessary.
6. Click **OK**.

Removing a column from the Product List

△ **CAUTION:** This procedure removes a column from the Product List without prompting you for a confirmation.

To remove unused Product List columns in a customized view:

1. Select **View > Edit View**.
2. Select the view you want to edit.

   The Edit View dialog box is displayed (Figure 43 on page 86).
3. Click the **Columns** tab.

   The Create View dialog box is displayed (Figure 42 on page 85).
4. Ensure the column you want to remove is listed in the Available Columns list. To move a column to the Available Columns list, select it in the Selected Columns list and click ◀.
5. Select the column you want to remove from the Available Columns list.
6. Click **Remove**.

4 Configuring SAN products and fabrics

This chapter provides instructions for configuring products, fabrics, and trap forwarding.

Managing SAN products

Use the HAFM application to manage discovered products.

Using the Element Manager

You can use the Element Manager to manage switches and directors directly from the HAFM application.

NOTE: Use only one copy of the application to monitor and manage the same devices in a subnet. Opening multiple copies of the application could result in errors.

Opening the Element Manager from the user interface

Use the Element Manager to search for a product, change product properties, and perform other configuration and maintenance tasks.

There are two ways to open the Element Manager from the HAFM user interface:

- Right-click a product icon and select **Element Manager**.
- Double-click a product icon.

Opening the Element Manager from the command line

The HAFM application contains a script that opens an Element Manager. To use the script:

1. Ensure that the HAFM appliance is running and the product is discovered.
2. Use a text editor to open the following script:

   `Install_Home\bin\HAFM_ElementMgr.bat.`
3. Under the heading, `rem HAFM Element Manager`, find the line that begins:

```
...ElementManagerStandAlone -s ServerIp -p ProductIp -u UserName -pw
Password
```

4. Enter the appropriate values for the following parameters:
   - ServerIp
   - ProductIp
   - UserName
   - Password

   Example:

   ```
   ...ElementManagerStandAlone -s 172.16.9.10 -p 172.16.9.211 -u Administrator
   -pw password
   ```
5. Save and close the file.
6. Run the script by double-clicking the file or entering the script name at a DOS prompt.

Searching for products in a SAN

You can search for a product in a SAN by entering a parameter in the search box on the toolbar.

1. Enter the search parameter (for example, an IP address) in the Search box on the HAFM toolbar.
2. Click the up or down arrow to search through the Physical Map.
3. Click **Search** to find each product.

NOTE: When the application finds a product, it highlights the product on the Physical Map as well as on the Product List.

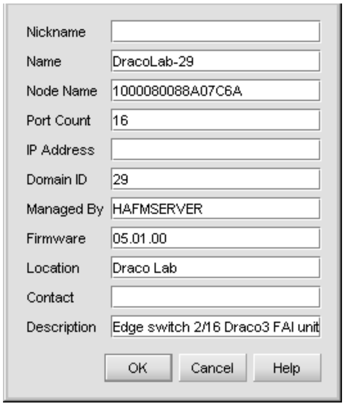
Changing product properties

You can change some of the properties of products that are online. This process does not change the product configuration.

To change product properties:

1. Right-click a product icon and select **Properties**.

   The Properties dialog box is displayed (Figure 46).



Nickname	
Name	DracoLab-29
Node Name	1000080088A07C6A
Port Count	16
IP Address	
Domain ID	29
Managed By	HAFMSERVER
Firmware	05.01.00
Location	Draco Lab
Contact	
Description	Edge switch 2/16 Draco3 FAI unit

Figure 46 Properties dialog box

NOTE: The product you select must be online for you to edit this information.

2. Edit the product properties as appropriate.
3. Click **OK**.

Determining product status

Determine product status by looking at the status icons on the Physical Map or the Product List. Table 15 describes the status icons.

Table 15 Product status icons

Icon	Status
No icon	Operational
⚠	Degraded
♦	Failed
▨	Unknown/Offline

Displaying service requests

To display a list of all products requiring attention, click the Attention Indicator icon (⚠) on the Status bar. The Service Request dialog box shows the names and IP addresses of all devices needing attention. Click a product name to jump to the product on the Physical Map. This list updates dynamically.

Displaying routes between ports

You can view the path that Fibre Channel frames must take between two ports in a multiswitch fabric. More than one route shows at a time within the same fabric. If you attempt to show a different route within the same fabric, the previous route fades.

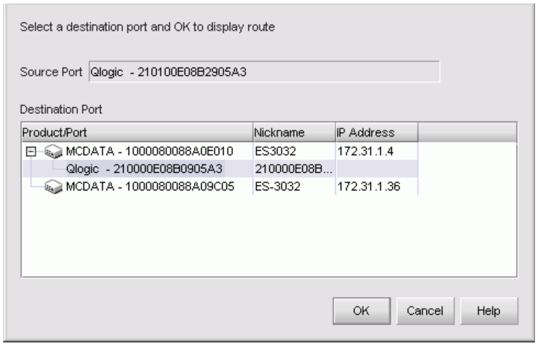
Before you display the route between two ports, ensure that:

- The fabric consists solely of HP M-series products.
- All switches or directors in the route are managed by the HAFM application and attached to the same appliance.
- All switches or directors in the route are attached to the same appliance.
- All switches or directors in the route are Director 2/64, Director 2/140, Edge Switch 2/32, Edge Switch 2/16, or Edge Switch 2/24 models and are running firmware 1.3 or higher.
- All attached products in the route are in the same zone.

To show the route for two ports:

1. In the Product List, click the plus **(+)** symbol next to the switch product icon you want to expand.
2. Right-click a node and select **Show Route**.

The Show Route dialog box is displayed (Figure 47).



Select a destination port and OK to display route

Source Port: Qlogic - 210100E08B2905A3

Destination Port

Product/Port	Nickname	IP Address
MCDATA - 1000080088A0E010	ES3032	172.31.1.4
Qlogic - 210000E08B0905A3	210000E08B...	
MCDATA - 1000080088A09C05	ES-3032	172.31.1.36

Figure 47 Show Route dialog box

3. Select a destination port from the Destination Port list.
4. Click **OK**.

   The route between the ports is displayed (Figure 48).

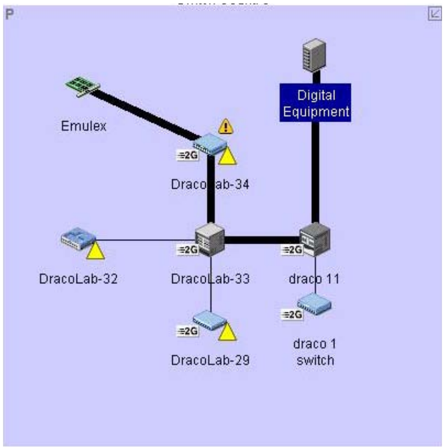


Figure 48 Displaying routes between ports

Hiding routes

You can hide routes between two ports in a multiswitch fabric.

To hide the route:

1. Display the route that you want to hide.

   See "Displaying routes between ports" on page 91.
2. Right-click the route and select **Hide Route**.

Displaying properties of routes

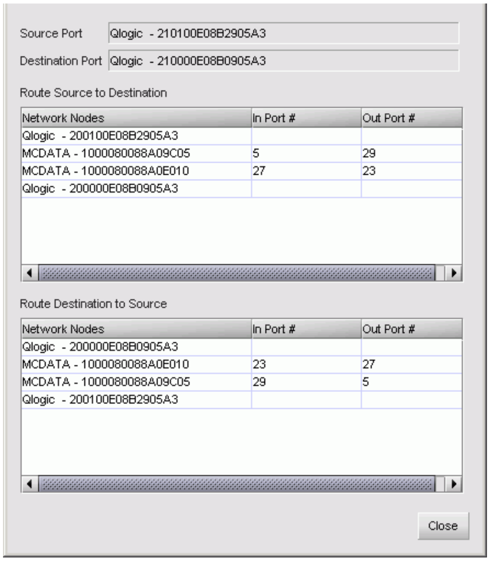
To display the properties of a route:

1. Display the route that you want to hide.

   See "Displaying routes between ports" on page 91.

2. Right-click the route and select **Properties**.

   The Route Properties dialog box is displayed (Figure 49).



Source Port: Qlogic - 210100E08B2905A3

Destination Port: Qlogic - 210000E08B0905A3

Route Source to Destination

Network Nodes	In Port #	Out Port #
Qlogic - 200100E08B2905A3		
MCDATA - 1000080088A09C05	5	29
MCDATA - 1000080088A0E010	27	23
Qlogic - 200000E08B0905A3		

Route Destination to Source

Network Nodes	In Port #	Out Port #
Qlogic - 200000E08B0905A3		
MCDATA - 1000080088A0E010	23	27
MCDATA - 1000080088A09C05	29	5
Qlogic - 200100E08B2905A3		

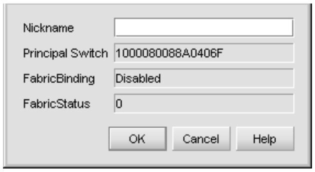
Figure 49 Route Properties dialog box

Displaying fabric properties

To display and change a fabric's properties:

1. Right-click a fabric icon or the background of an expanded fabric and select **Properties**.

   The Fabric Properties dialog box is displayed (Figure 50).



Nickname:

Principal Switch: 1000080088A0406F

FabricBinding: Disabled

FabricStatus: 0

Figure 50 Fabric Properties dialog box

The nickname is the only fabric property that can be changed. Assigning a nickname to a fabric is optional. However you cannot revert to having no nickname after one has been assigned. You can change the nickname if you choose, but you cannot leave the Nickname box blank after assigning a nickname.

Configuring Enterprise Fabric Mode

Enterprise Fabric Mode option automatically enables features and operating parameters in multiswitch enterprise fabric environments. Enabling Enterprise Fabric Mode forces each switch in the fabric to enforce the following security-related features:

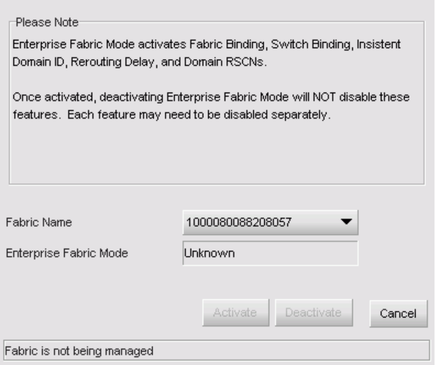
- **Fabric Binding**—Allows or prohibits switches from merging with a selected fabric.
- **Switch Binding**—Allows or prohibits switches from connecting to switch E_Ports and F_Ports.
- **Rerouting delay**—Ensures that frames are delivered through the fabric in order to their destination, even if a shorter, new path is created. Frames sent over the new, shorter path are delayed to arrive after older frames still in route over the older path.
- **Domain register state change notifications (RSCNs)**—Indicates a switch entered or left the fabric. Notifications occur fabric-wide and do not have zoning constraints.
- **Insistent domain ID**—Sets the domain ID as the active domain identification when the fabric initializes. If insistent domain ID is enabled, the switch isolates itself from the fabric if the preferred domain ID is not the switch's domain ID.

Enabling and disabling Enterprise Fabric Mode

To enable or disable Enterprise Fabric Mode for a fabric:

1. Select **Configure > Enterprise Fabric Mode**.

   The Enterprise Fabric Mode dialog box is displayed (Figure 51).



Please Note

Enterprise Fabric Mode activates Fabric Binding, Switch Binding, Insistent Domain ID, Rerouting Delay, and Domain RSCNs.

Once activated, deactivating Enterprise Fabric Mode will NOT disable these features. Each feature may need to be disabled separately.

Fabric Name: 1000080088208057

Enterprise Fabric Mode: Unknown

Fabric is not being managed

Figure 51 Enterprise Fabric Mode dialog box

2. Select the fabric for which you want to configure Enterprise Fabric Mode from the Fabric Name list.

   The fabric's current status is displayed in the Enterprise Fabric Mode box.
3. To enable Enterprise Fabric Mode on the selected fabric, click **Activate**. To disable Enterprise Fabric Mode on the selected fabric, click **Deactivate**.

NOTE: You must be managing the fabric in order to disable Enterprise Fabric Mode.

Configuring Fabric Binding

Fabric Binding enables you to configure whether switches can merge with a selected fabric. This provides security from accidental fabric merges and potential fabric disruption.

Fabric Binding requires the installation of a security feature called SANtegrity. See "SANtegrity features" on page 118 for details.

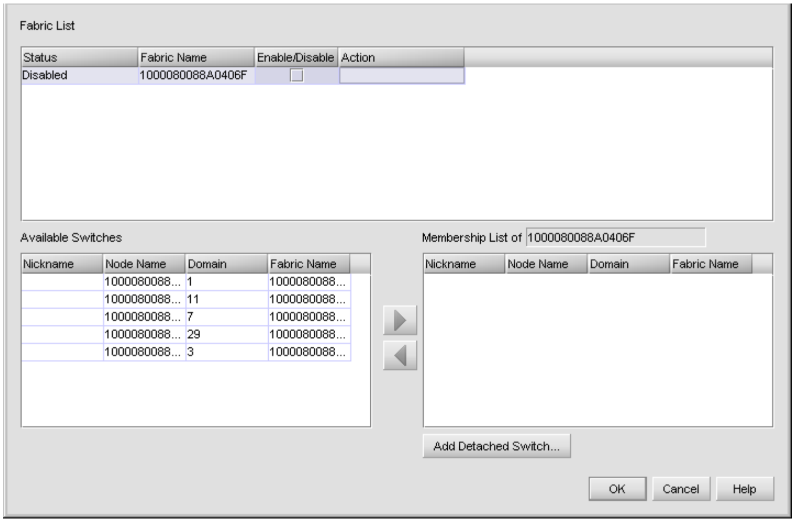
NOTE: You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled.

Enabling Fabric Binding

You enable Fabric Binding using the Fabric Binding dialog box. After you enable Fabric Binding, use the Membership List to add switches that you want to allow in the fabric.

1. Select **Configure > Fabric Binding**.

   The Fabric Binding dialog box is displayed (Figure 52).



Fabric List

Status	Fabric Name	Enable/Disable	Action
Disabled	1000080088A0406F	□	

Available Switches

Nickname	Node Name	Domain	Fabric Name
	1000080088...	1	1000080088...
	1000080088...	11	1000080088...
	1000080088...	7	1000080088...
	1000080088...	29	1000080088...
	1000080088...	3	1000080088...

Membership List of 1000080088A0406F

Nickname	Node Name	Domain	Fabric Name

Figure 52 Fabric Binding dialog box

2. Select the **Enable/Disable** check box for the fabric for which you want to configure Fabric Binding.
3. Click **OK**.

Adding and removing switches

With Fabric Binding enabled, you can add or remove switches from the membership list.

- To add switches to the selected fabric's membership list, select the switches from the Available Switches list in the Fabric Binding dialog box, and click ▶ to move the switches to the membership list.
- To add a switch that does not have physical connection to the fabric:
  - **a.** Click **Add Detached Switch**.
  - **b.** Enter the appropriate information in the following boxes:
    - Domain ID
    - Node WWN
  - **c.** Click **OK**.
- To remove switches from the selected fabric's membership list, select the switches from the Membership List in the Fabric Binding dialog box. Click ◀ to move the switches to the Available Switches list.

Persisting and unpersisting fabrics

When you persist a fabric, you take a snapshot of the fabric's products and connections. This serves as a reference point for future comparisons. You can export the persisted fabric information for future reference. See "Exporting data" on page 52.

NOTE: Each fabric has an HP principal switch to manage the devices in fabric. If the principal switch changes, the new fabric must be manually persisted.

Persisting a fabric

To persist a fabric from the HAFM main window, do one of the following:

- Select a fabric in the Physical Map or Product List, and then select **Configure > Persist Fabric**.
- Right-click the fabric in the Physical Map or Product List, and then select **Persist Fabric**.
- Highlight a fabric in the Physical Map or Product List, and then click the **Persist Fabric** icon on the toolbar.

Unpersisting a fabric

To unpersist a fabric from the HAFM window, do one of the following:

- Highlight a fabric in the Physical Map or Product List, and then select **Configure > Unpersist Fabric**.
- Right-click the fabric in the Physical Map or Product List, and then select **Unpersist Fabric**.

  A confirmation box is displayed, and then click **OK**.

Unpersisting a product

You can unpersist a product that is no longer part of a persisted fabric. Doing so removes all connections associated with that product and updates the persisted fabric's data.

To unpersist a product, from the HAFM main window:

1. Right-click the product in the Physical Map or Product List, and then select **Unpersist Fabric.**

   A confirmation box is displayed.
2. Click **OK**.

Interpreting status

There are various ways to determine the status of persisted fabrics and products. Real-time changes to the fabric display on the Physical Map and the Product List and are listed in the fabric log.

Persisted fabric status

The green circle indicator on the fabric icon on the Physical Map and in the Product List shows the fabric is persisted (Figure 53).

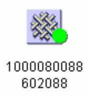


Figure 53 Persisted fabric icon on Physical Map

The Fabric Log lists changes to the persisted fabric. For details about the fabric log, see "Monitoring events" on page 101.

Product status

When you add a product to a persisted fabric, is displayed with a plus (+) icon (Figure 54).

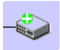


Figure 54 Product added to persisted fabric

When you remove a product from a persisted fabric, it is displayed as a ghost image with a minus (-) icon (Figure 55). To find a product that is removed from a persisted fabric, right-click the ghost image, and then select **Find Product**. The corresponding online item is displayed.

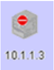


Figure 55 Product removed from persisted fabric

Connection status

If more than one connection exists between products, the Physical Map shows connection status as follows:

- If all connections are enabled, they display as black lines.
- If all connections are disabled, they display as yellow dashed lines.
- If one or some of the connections are disabled (but not all), the enabled connections display as black lines and the disabled connections display as yellow, dashed lines with an interswitch link (ISL) alert (Figure 56).

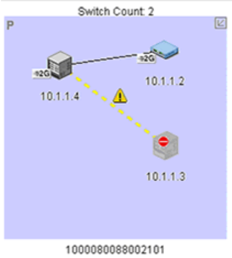


Figure 56 Removed connection in a persisted fabric

Clear ISLs from the Physical Map as follows:

- To clear an ISL alert, right-click the ISL icon and select **Clear ISL Alerts**.
- To clear all ISL alerts, select **Edit > Clear All ISL Alerts**.

Changing persisted fabrics

When you merge two persisted fabrics, the fabric whose principal switch is also the principal switch in the merged fabric becomes the *real* fabric. It includes the switches of both fabrics in the Physical Map and the Product List. The other fabric becomes a *ghost* fabric.

On the Physical Map, the ghost fabric shows its original products with minus symbols (Figure 55). On the Product List, the ghost fabric is shown as offline without products. The fabric log resets after the fabrics merge.

When you split merged fabrics, the fabric that includes the principal switch becomes the persisted fabric.

When you move a product in a persisted fabric's topology, the new location is stored on the client. If the updated fabric is not persisted, users logged in from a different client can show an invalid layout.

Configuring trap forwarding

Trap forwarding enables you to configure the application to send SNMP traps to other computers. To configure trap reporting, you must configure the target computer's IP address and SNMP ports:

1. Select **Monitor > Trap Forwarding**.

The Configure Trap Forwarding dialog box is displayed (Figure 57).

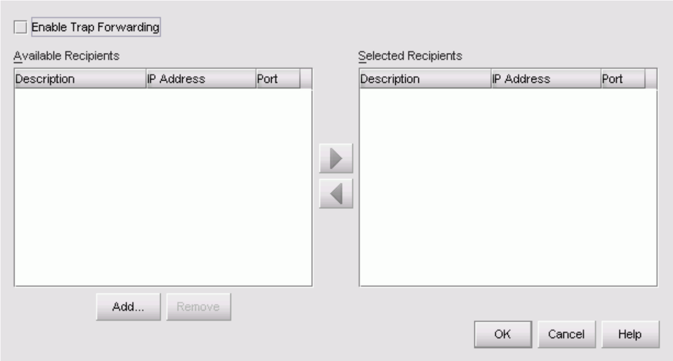


Figure 57 Configure Trap Forwarding dialog box

2. If necessary, add trap recipients to the Available Recipients list.

   See "Adding trap recipients" on page 99 for instructions.
3. Select the recipient that you want to provide trap messages to in the Available Recipients list.
4. Click the right arrow button.
5. Scan the Selected Recipients list, and, if necessary, select recipients to move from the list and then click left arrow button.
6. Select the **Enable Trap Forwarding** check box.
7. Click **OK**.

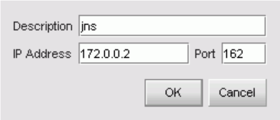
Adding trap recipients

To add a trap recipient:

1. Select **Monitor > Trap Forwarding**.

   The Configure Trap Forwarding dialog box is displayed (Figure 57).
2. Click **Add**.

   The Add Trap Recipient dialog box is displayed (Figure 58).



Description jns
IP Address 172.0.0.2
Port 162

Figure 58 Add Trap Recipient dialog box

3. Enter the appropriate information in the following boxes:
   - Description
   - IP Address
   - Port

NOTE: The HAFM appliance interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, firmware versions 4.0 and below send the actual port number and firmware versions 5.X and above add one to the port number to match the specification. However, third party applications cannot correctly interpret the information.

4. Click **OK** to close the Add Trap Recipient dialog box.
5. Click **OK** to close the Configure Trap Forwarding dialog box.

Removing trap recipients

To remove a trap recipient:

1. Select **Monitor > Trap Forwarding**.

   The Configure Trap Forwarding dialog box is displayed (Figure 57).
2. Highlight the recipient you want to remove from the Available Recipients list.
3. Click **Remove**.
4. Click **OK**.

5 Monitoring SAN products

This chapter contains the following topics, which describe the tools you can use to monitor SAN products.

- Monitoring events, page 101
- Using event notifications, page 104
- Creating reports, page 106

Monitoring events

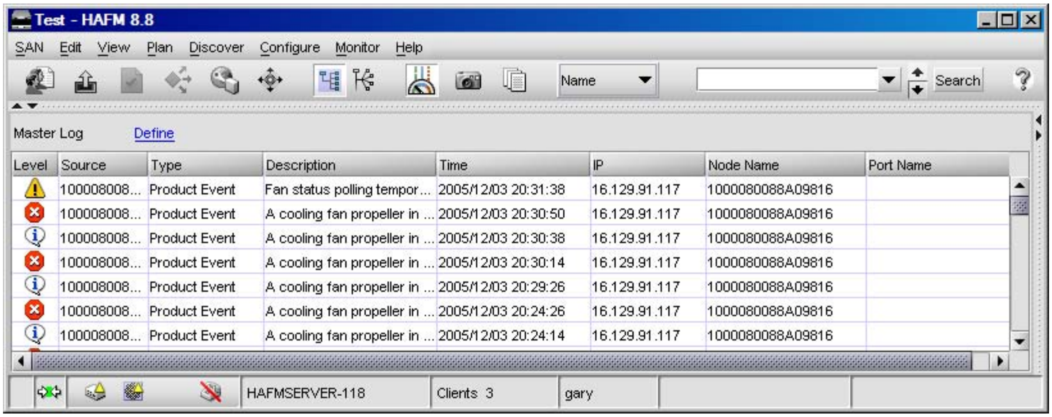
The HAFM application provides logs that you can use to monitor SAN products. You can view all events or specify which events you want to view. The available logs include:

- **Master Log**—Lists all SAN events
- **Audit Log**—Lists a history of user actions (except log in/log out)
- **Event Log**—Lists errors related to SNMP traps and client-server communications
- **Fabric Log**—Lists a history of changes to the fabric including:
  - ISL added to fabric
  - ISL removed from fabric
  - Switch added to fabric
  - Switch removed from fabric
  - Fabric renamed
  - Fabric persisted
  - Fabric status changed
  - Device unpersisted
- **Group Log**—Lists the event logs defined using the Group Manager window.
- **Security Log**—Lists the following security information:
  - Severity
  - User
  - Reason
  - Description
  - Date and Time
  - Count
  - Category
  - IP
  - Role
  - Interface
- **Session Log**—Lists users who have logged in and out of the HAFM appliance
- **Product state Log**—Lists status changes for managed products

The application also has an event notification feature. Configure event notification to specify when the application notifies users of an event. See "Using event notifications" on page 104 for details.

Viewing the Master Log

The main HAFM window displays the Master Log (Figure 59). It provides detailed information about all SAN events. If the Master Log is not displayed in the main window, select **View > All Panels**.



Level	Source	Type	Description	Time	IP	Node Name	Port Name
⚠	100008008...	Product Event	Fan status polling tempor...	2005/12/03 20:31:38	16.129.91.117	1000080088A09816	
✖	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:30:50	16.129.91.117	1000080088A09816	
ℹ	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:30:38	16.129.91.117	1000080088A09816	
✖	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:30:14	16.129.91.117	1000080088A09816	
ℹ	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:29:26	16.129.91.117	1000080088A09816	
✖	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:24:26	16.129.91.117	1000080088A09816	
ℹ	100008008...	Product Event	A cooling fan propeller in ...	2005/12/03 20:24:14	16.129.91.117	1000080088A09816	

HAFMSERVER-118 | Clients 3 | gary

Figure 59 Master log

The Master Log columns are:

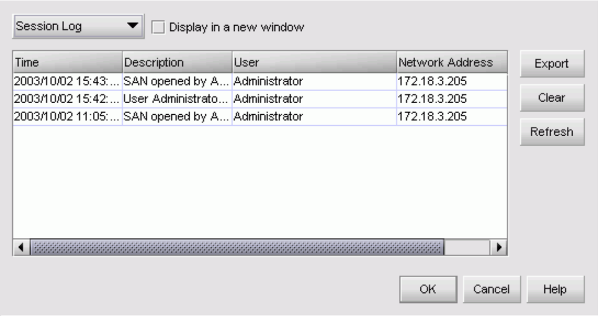
- **Level**—The level of the event:
  - Informational
  - Warning
  - Fatal
- **Source**—The product on which the event occurred
- **Type**—The type of event (for example, client-server communication events)
- **Description**—Description of the event
- **Time**—The time and date on which the event occurred
- **IP**—The IP address of the product on which the event occurred
- **Node Name**—The name of the node on which the event occurred
- **Port Name**—The name of the port on which the event occurred

Viewing other logs

If you want to view certain types of events, but not the entire event log, you can open a specific log. To view more than one log, you must open a separate window for each.

1. Select **Monitor > Logs**.

The View Logs dialog box is displayed (Figure 60).



Session Log

□ Display in a new window

Time	Description	User	Network Address
2003/10/02 15:43:...	SAN opened by A...	Administrator	172.18.3.205
2003/10/02 15:42:...	User Administrato...	Administrator	172.18.3.205
2003/10/02 11:05:...	SAN opened by A...	Administrator	172.18.3.205

Figure 60 View Logs dialog box

2. Select the log that you want to view.
3. If you want to view multiple logs simultaneously, select the **Display in a new window** check box and then select an additional log.
    - To clear the selected log, click **Clear**.
    - To refresh the selected log, click **Refresh**.
4. Click **OK**.

Exporting log data

You can export HAFM log data in tab-delimited format. This feature is useful if you want to provide the data to a third party or include it in a report.

1. Select the log you want to export from the View Logs dialog box (Figure 60).
2. Click **Export**.

    The Save dialog box is displayed.
3. Browse to the folder where you want to save the file.
4. Enter a file name in the File Name box.
5. Click **Save**.

To view the exported file in table format, open the file in Microsoft Excel.

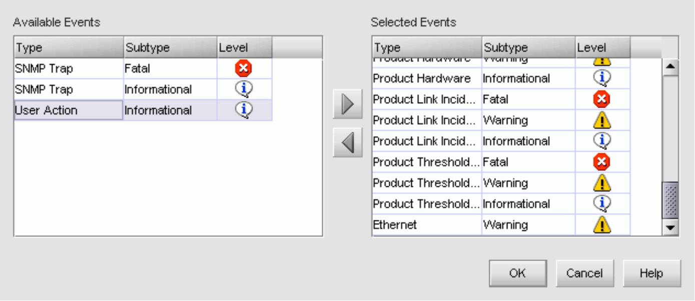
See "Exporting and importing data" on page 51 for more information.

Filtering events in the Master Log

To filter the events that display in the Master Log:

1. Click the **Define** link in the Master Log.

The Define Filter dialog box is displayed (Figure 61).



Available Events

Type	Subtype	Level
SNMP Trap	Fatal	✖
SNMP Trap	Informational	ⓘ
User Action	Informational	ⓘ

Selected Events

Type	Subtype	Level
Product Hardware	Informational	ⓘ
Product Link Incid...	Fatal	✖
Product Link Incid...	Warning	⚠
Product Link Incid...	Informational	ⓘ
Product Threshold...	Fatal	✖
Product Threshold...	Warning	⚠
Product Threshold...	Informational	ⓘ
Ethernet	Warning	⚠

Figure 61 Define Filter dialog box

2. Select the events from the Available Events list that you want to include in the Master Log.
3. Click ▷.
4. Scan the Selected Events list and select any event you want to exclude from the Master Log.
5. Click ◁.
6. Click **OK**.

Copying log entries

Use the cut (**Ctrl-C**) and paste (**Ctrl-V**) features to copy data and column headings from logs to other applications. Use the copy all (**Ctrl-A**) feature to select all from the menu.

NOTE: When using the View Logs dialog box, you can copy only one row at a time. To copy multiple rows of data, copy the data from the Master Log on the HAFM main window.

Using event notifications

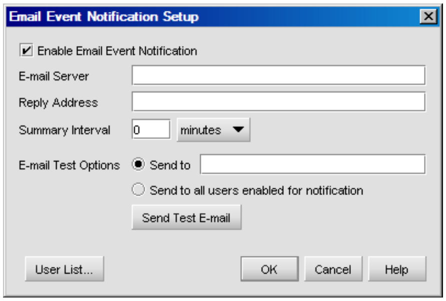
You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of SAN events. You can also configure products to Call Home to notify the support center of product problems.

Configuring e-mail notification

To configure e-mail notification:

1. Select **Monitor > Event Notification > Email**.

The Email Event Notification Setup dialog box is displayed (Figure 62).



Email Event Notification Setup

☑ Enable Email Event Notification

E-mail Server

Reply Address

Summary Interval 0 minutes

E-mail Test Options ● Send to

○ Send to all users enabled for notification

Figure 62 Email Event Notification Setup dialog box

2. Select the **Enable Email Event Notification** check box.
3. Enter the appropriate information in the following boxes:
    - **E-mail Server**—IP address or name of the SMTP server
    - **Reply Address**—Recipient's e-mail address
    - **Summary Interval**—Amount of time between each notification

△ **CAUTION:** Specifying a short interval can cause the recipient's e-mail inbox to fill quickly.

4. Select one of the following options:
    - Select **Send to** and enter an e-mail address for a user to send a test e-mail to a specific user.
    - Select **Send to all users enabled for notification** to send a test e-mail to all users designated to receive notification.
5. Click **Send Test Email** to test the e-mail server.

   A message is displayed indicating if the server was found.
6. Click **User List** to specify which users receive e-mail notifications.

   The HAFM Server Users dialog box is displayed.
7. Select the check box in the Email column for each user you want to receive notification.
8. Click **OK**.

Notifications are combined into a single e-mail and sent at the specified interval setting. An interval setting of 0 (zero) causes notifications to be sent immediately.

Configuring Call Home notification

When you configure Call Home notification, the appliance automatically dials in to a support center to report system problems. See the *HA-Fabric Manager Appliance installation guide* for details.

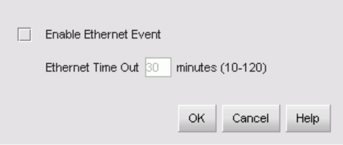
Enabling Ethernet events

An Ethernet event occurs when the Ethernet link between the appliance and the managed product is lost.

To enable Ethernet events notification:

1. Select **Monitor > Ethernet Event**.

   The Configure Ethernet Event dialog box is displayed (Figure 63).



□ Enable Ethernet Event

Ethernet Time Out 30 minutes (10-120)

Figure 63 Configure Ethernet Event dialog box

2. Select the **Enable Ethernet Event** check box.
3. Enter the amount of time between the event and the notification in the Ethernet Time Out box.
4. Click **OK**.

Creating reports

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following report types are available:

- **Product List**—Lists the Product List, which has detailed information about the products in the SAN.
- **Operating Status Change**—Lists status change for products in the SAN, including the number of products online and offline, the product with the most downtime, and details about each product's status. This report only captures events from the event log for the last 30 days. To save space, the log can be truncated and events lost, resulting in an inaccurate summary.
- **Performance Data**—Displays the performance data. The Performance Module is an optional feature. Contact your sales representative to purchase this module.
- **Physical Map**—Displays a graphic of the SANs topology.
- **Port Usage**—Lists the number of connected ports in the SAN, as well as detailed usage information for each port. Since only E_Ports are displayed in the topology, they are the only ports displayed in this report.
- **Fabric Ports**—Lists fabric details including port and director utilization and product data.
- **Storage Device Summary**—Lists the assigned and free LUNs for the storage being managed through the application.
- **LUN Masking Summary**—Lists the number of host ports and storage devices in the SAN, as well as the nicknames of hosts that do not have assigned LUNs.

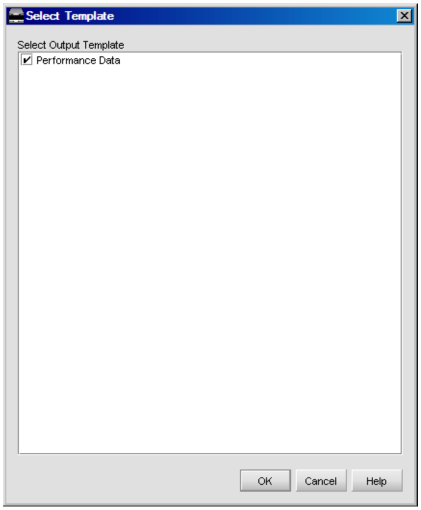
- **Departmental Storage Allocation**—Lists the storage allocation for the entire SAN, as well as the number of servers on the SAN for each department, number of unique LUNs assigned to those servers, total size of those unique LUNs, and total percentage for each department. You must have the LUN Management module to generate this report. This is an optional feature. Contact your sales representative to purchase the module.

Generating reports

You can generate various SAN report. Generated reports are saved to *`Install_Home\Server\Reports\`*.

1. Select **Monitor > Reports > Generate**.

   The Select Template dialog box is displayed (Figure 64).



Select Output Template

☑ Performance Data

Figure 64 Select Template dialog box

NOTE: You can generate a report of the Physical Map by clicking **Generate Reports** (or pressing **Ctrl-G**) on the right-hand toolbox while viewing a discovered SAN.

2. Select the type(s) of reports you want to generate.
3. Click **OK**.

   The generated reports are automatically displayed in the Reports dialog box.
4. To print the report:
   - **a.** Click **Show in Browser**.

     The selected report is displayed in your default web browser.
   - **b.** Select **File > Print** in the web browser.
   - **c.** Close the web browser and the Reports dialog box.

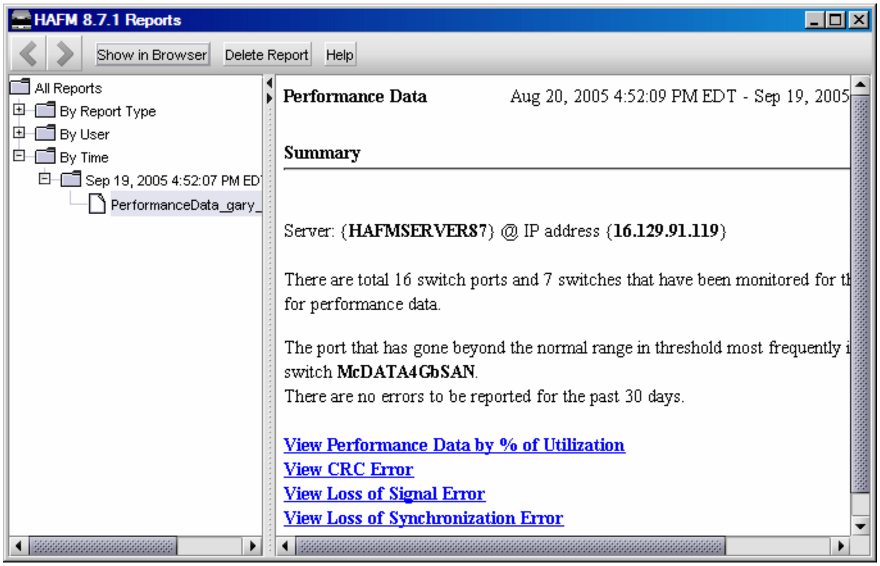
NOTE: Hyperlinks in reports are active as long as the source data is available.

Viewing reports

You can view reports through the application or through a web browser. Reports are stored in *`Install_Home\Server\Reports\`*.

1. Select **Monitor > Reports > View**.

   The Reports dialog box is displayed (Figure 65).



Performance Data Aug 20, 2005 4:52:09 PM EDT - Sep 19, 2005

Summary

Server: {**HAFMSERVER87**} @ IP address {**16.129.91.119**}

There are total 16 switch ports and 7 switches that have been monitored for th for performance data.

The port that has gone beyond the normal range in threshold most frequently i switch **McDATA4GbSAN**.
There are no errors to be reported for the past 30 days.

View Performance Data by % of Utilization
View CRC Error
View Loss of Signal Error
View Loss of Synchronization Error

Figure 65 Reports dialog box

2. Select the report you want to view from the left-hand pane.

   If you don't see the report you want to view, generate it first by following the instructions in "Generating reports" on page 107.

NOTE: Hyperlinks in reports are active as long as the source data is available.

3. To print the report:
   a. Click **Show in Browser**.

      The selected report is displayed in your default web browser.
   b. Select **File > Print** in the web browser.
   c. Close the web browser and the Reports dialog box.

Deleting reports

To delete reports:

1. Select **Monitor > Reports > View**.

   The Reports dialog box is displayed (Figure 65).
2. Select the report(s) you want to delete.
3. Click **Delete Report**.

   The report is deleted without confirmation.
4. Close the Reports dialog box.

6 Optional HAFM features

This chapter provides detailed information on using, administering, and configuring optional HAFM features. There are two types of features:

- Keyed features that require the purchase of feature keys
- Features that do not require feature keys, but do require separate keyed features

This chapter describes the following topics:

- Feature keys, page 111
- Event Management, page 112
- SANtegrity features, page 118
- Open trunking, page 130
- Performance Module, page 133
- Planning Module, page 136

Feature keys

Certain HAFM optional features require the installation of a feature key to validate ownership. See the *HP StorageWorks HA-Fabric Manager Appliance installation guide* for more information about feature keys.

To install and enable a feature key:

1. Obtain the feature key.
2. Select **Configure > Features** from the Element Manager window.

   The Configure Feature Key dialog box is displayed (Figure 66).

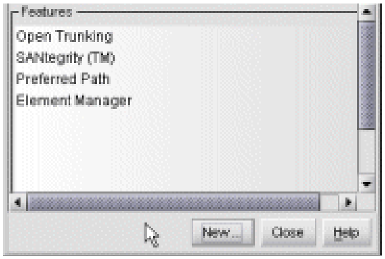


Figure 66 Configure Feature Key dialog box

3. Click **New**.

   The New Feature Key dialog box is displayed (Figure 67).

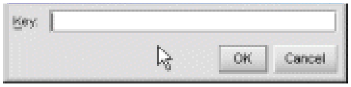


Figure 67 New Feature Key dialog box

4. Enter the feature key in the Key box.
5. Click **OK**.

Event Management

Event Management automates tasks that are performed on the SAN. You can configure the application to automatically perform functions, such as:

- Sending an e-mail notification when events or errors occur
- Generating reports at specific times or for specific reasons
- Exporting data
- Playing sounds for notification of events

Components

The Event Management feature uses *triggers* and *actions* to create rules which determine when and why SAN tasks are automatically executed.

Triggers

Triggers define the condition that causes the action to occur or *fire*. There are two types of triggers:

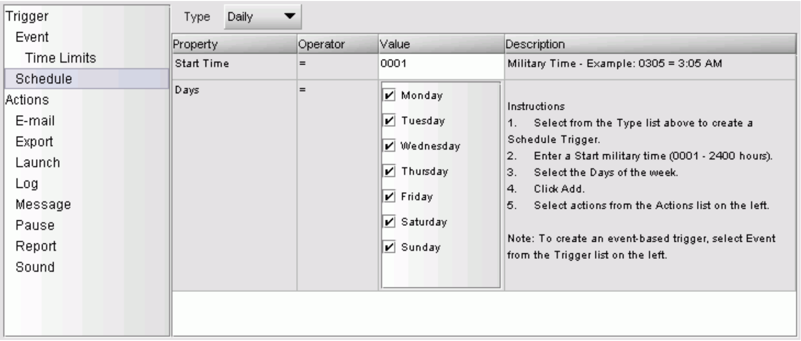
- Event triggers, page 114
- Schedule triggers, page 114

Both trigger types are comprised of logically-related phrases, and each phrase is composed of three parts:

- **Property**—A variable for which you are setting values. There are many types of property variables. See "Reference" on page 267.
- **Operator**—Defines the relationship between properties and their values. Table 16 lists the available trigger operators. Multiple operators can be defined, and phrase operators describe the relationship between them.
- **Value**—A user-defined value, presented in a list or entered by the user.

NOTE: Once you have selected a trigger type, you can select only options within that type to complete the trigger phrase.

Figure 68 shows the dialog box you use to create a trigger phrase.



Type Daily

Property	Operator	Value	Description
Start Time	=	0001	Military Time - Example: 0305 = 3:05 AM
Days	=	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday	Instructions 1. Select from the Type list above to create a Schedule Trigger. 2. Enter a Start military time (0001 - 2400 hours). 3. Select the Days of the week. 4. Click Add. 5. Select actions from the Actions list on the left. Note: To create an event-based trigger, select Event from the Trigger list on the left.

Figure 68 Trigger phrase development

Table 16 Trigger operators

Operator	Value
==	Number
!=	Number
<	Number
<=	Number
>	Number
>=	Number
Contains	String
Does Not Contain	String
Starts With	String
Ends With	String

Phrase operators

If the rule states that more than one operator must apply, phrase operators describe the relationship between them. The following phrase operators are used:

- AND
- OR
- AND NOT
- OR NOT

Event triggers

Event triggers monitor system events and fire when the specified conditions exist. You can define the phrases (rows) and their logical relationships. The phrases filter all the event context properties to identify those events that you want to trigger the event.

Event triggers also allow you to set time limits so that the trigger occurs only if the event happens within a certain time and date range. For example, you can specify that all offline events between 5 p.m. and 8 a.m. trigger e-mail message and log actions to take place.

Schedule triggers

Schedule triggers monitor the system clock and fire when the specified time and date conditions are met.

Schedule triggers can be set to fire:

- Daily
- Weekly
- Monthly
- One time only
- Hourly

△ **CAUTION:** Once you have chosen a schedule type and added the first phrase, do not change types or you can lose your work.

Actions

You can configure multiple actions to be performed when the specified triggers are fired.

The following actions are possible:

- **E-mail**—Send an e-mail to specified recipients.
- **Export**—Export data.
- **Launch**—Launch an application using a script.
- **Log**—Add an entry to the Master Log file and window display.
- **Message**—Display a message to all open clients.
- **Pause**—Insert a pause between actions.
- **Report**—Generate a report.
- **Sound**—Play a sound.

The launch and sound actions point to information in a file. You can select an existing option from a list, or add options to the list as follows:

- For a launch action, add your script files to the `Install_Home\Server\LaunchScripts` directory.
- For a sound action, add your sounds to the `Install_Home\Server\Sounds` directory.

📝 **NOTE:** You can specify macros for some actions by clicking in the Value column and then right-clicking and selecting an argument from the menu. See ″Writing Event Management macros″ on page 277 for instructions.

Window

To view Event Management, click the Event Management tab on the HAFM main window. All configured rules display (Figure 69). From this dialog box, you can manage Event Management rules. See Table 17 for a description of each window section.

Table 17 Event Management tab

Window section	Description
# column	Specifies the auto-assigned rule number.
Actions list	Lists the actions to be performed when the rule’s triggers are met.
Activate button	Click to activate the selected rules.
Active column	Specifies whether the rule is on.
Change button	Click to change the reset interval.
Copy button	Click to duplicate the selected rule.
Date Modified column	Lists the date and time that the rule was last edited.
Deactivate button	Click to deactivate the selected rules.
Delete button	Click to delete the selected rule.
Description box	Lists the description of the selected rule.
Description column	Specifies the user-defined rule description.
Edit button	Click to edit the selected rule.
Group column	Lists the group to which the rule belongs.
Name column	Specifies the user-defined rule name.
New button	Click to add a new rule.
OFF button	Click to turn the Event Management feature off.
ON button	Click to turn the Event Management feature on.
Trigger list	Lists the trigger for the selected rule.
User column	Specifies the last user to modify the rule.

Rules

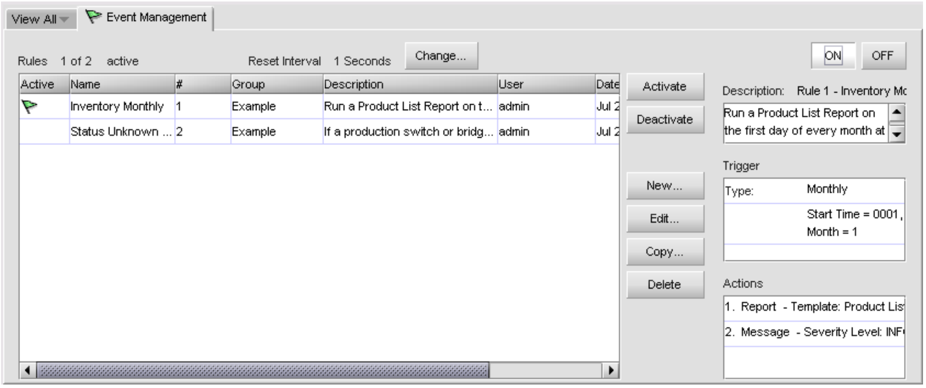
This section provides instructions for writing rules and setting up automated tasks. Before you begin, decide which triggers, actions, and schedules you want the rule to follow. For more information, see:

- "Triggers" on page 112
- "Actions" on page 114
- "Schedule triggers" on page 114

Creating a rule

To create a rule:

1. Click the Event Management tab on the HAFM main window to display Event Management information (Figure 69).



Rules 1 of 2 active

Reset Interval 1 Seconds

Active	Name	#	Group	Description	User	Date
✓	Inventory Monthly	1	Example	Run a Product List Report on t...	admin	Jul 2
	Status Unknown ...	2	Example	If a production switch or bridg...	admin	Jul 2

Description: Rule 1 - Inventory Mc

Run a Product List Report on the first day of every month at

Trigger

Type: Monthly

Start Time = 0001 , Month = 1

Actions

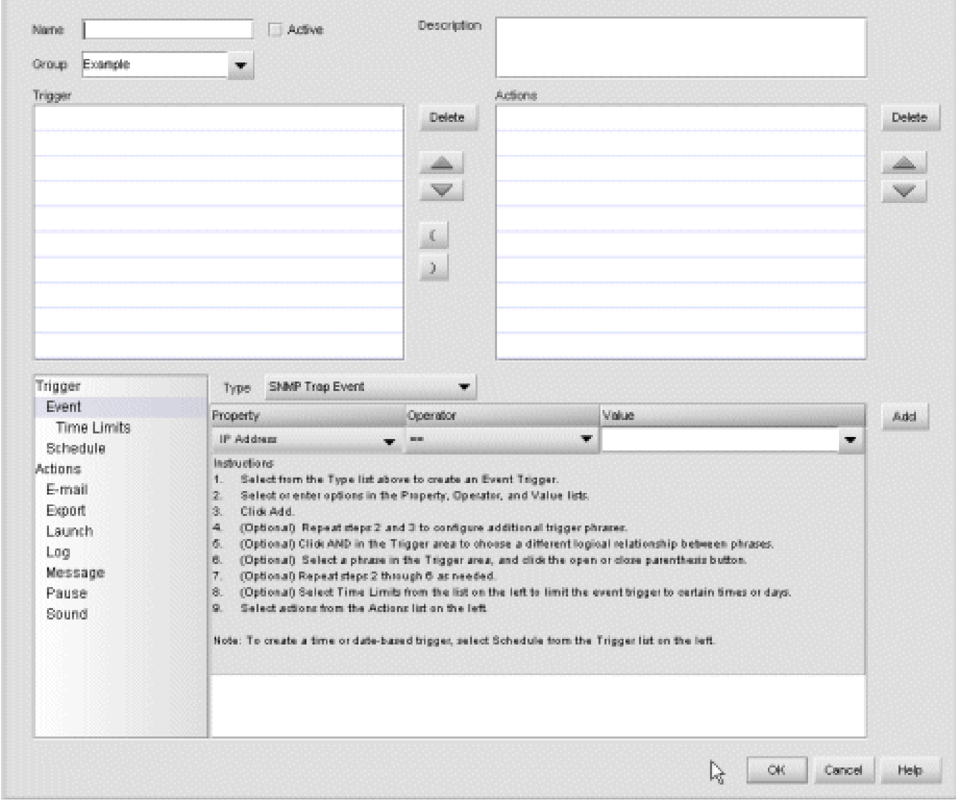
1. Report - Template: Product Lis

2. Message - Severity Level: INF

Figure 69 Event Management tab

2. Click **New**.

The Add Rule dialog box is displayed (Figure 70).



Group: Example

Type: SNMP Trap Event

Property: IP Address

Operator: ==

Instructions

1. Select from the Type list above to create an Event Trigger.
2. Select or enter options in the Property, Operator, and Value lists.
3. Click Add.
4. (Optional) Repeat steps 2 and 3 to configure additional trigger phrases.
5. (Optional) Click AND in the Trigger area to choose a different logical relationship between phrases.
6. (Optional) Select a phrase in the Trigger area, and click the open or close parenthesis button.
7. (Optional) Repeat steps 2 through 6 as needed.
8. (Optional) Select Time Limits from the list on the left to limit the event trigger to certain times or days.
9. Select actions from the Actions list on the left.

Note: To create a time or date-based trigger, select Schedule from the Trigger list on the left.

Figure 70 Add Rule dialog box

3. Enter information in the following boxes:
   - Name
   - Group
   - Description
4. Select the **Active** check box to make the rule active after you are finished creating it.
5. Select the type of trigger from the Trigger list.
6. Follow the instructions on the window.

NOTE: Each selection on the Trigger list or Actions list shows a different dialog box with instructions. Follow the instructions on each dialog box to create rules.

Managing Event Management

You can turn Event Management on or off by clicking the on or off button on the top right corner or the Event Management tab.

Also from the Event Management tab, you can manage the Event Management rules. Select a rule and then click the appropriate button to:

- Activate the selected rule
- Deactivate the selected rule
- Edit the selected rule
- Copy the selected rule
- Delete the selected rule

SANtegrity features

SANtegrity includes a set of features that enhance security in Storage Area Networks (SANs) that contain a large and mixed group of fabrics and attached devices. Through these features you can allow or prohibit switch attachment to fabrics and device attachment to switches. These features are enabled by purchasing a feature key, then enabling the key through the Configure Feature Key dialog box.

SANtegrity Binding features include:

- Fabric Binding
- Switch Binding

Although Enterprise Fabric Mode is not a keyed feature, the SANtegrity Fabric Binding and Switch Binding must be installed before you can use the Enterprise Fabric Mode function through the HAFM Fabrics menu.

Fabric Binding

This feature is managed through the Fabric Binding option, available through the Fabrics menu in HAFM when the Fabrics tab is selected. Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Enable/disable and online state functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by WWN and domain ID, the Insistent Domain ID option in the Configure Switch Parameters dialog box is automatically enabled if Fabric Binding is enabled.
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director or switch is offline, you can disable Insistent Domain ID, but this disables Fabric Binding.
- You cannot disable Fabric Binding or Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.

Switch Binding

This feature is managed through the Switch Binding option, available on the Element Manager Configure menu. Using Switch Binding, you can specify devices and switches that can attach to director and switch ports. This provides security in environments that include a large number of devices by ensuring that only the intended set of devices attach to a switch or director.

Overview

To configure Switch Binding, you must first activate the feature using the Switch Binding – State Change dialog box while selecting the type of port where you want to restrict connection (connection policy). Possible selections are E_Ports, F_Ports, or all types.

If the director or switch is online, activating Switch Binding populates the Membership List in the Switch Binding - Membership List dialog box (Element Manager) with the following WWNs currently connected to the director or switch, depending on the connection policy set in the Switch Binding – State Change dialog box:

- WWNs of devices connected to F_Ports (F_Port connection policy). The WWN is the WWN of the attached device's port.
- WWNs of switches connected to E_Ports (E_Port connection policy). The WWN is the WWN of the attached switch.
- WWNs of devices connected to F_Ports and switches connected to E_Ports (all-ports connection policy).

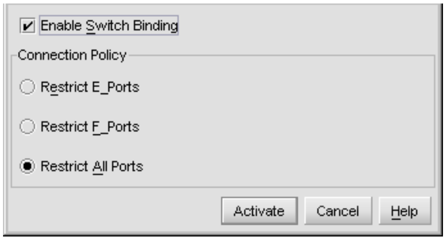
When the Switch Binding feature is first installed and has not been enabled, the Switch Membership List is empty. When you enable Switch Binding, the Membership List is populated with WWNs of devices, switches, or both that are currently connected to the switch. If the switch is offline and you activate Switch Binding, the Membership List is not automatically populated. Edits to the Switch Binding Membership list are maintained when you enable or disable Switch Binding.

After enabling Switch Binding, you prohibit devices and switches from connecting with director or switch ports by removing them from the Membership List in the Switch Binding – Membership List dialog box. You allow connections by adding them to the Membership List. You can also add detached nodes and switches.

Enabling/disabling Switch Binding

Use the following procedure to enable and disable Switch Binding:

1. Select **Configure > Switch Binding > Change State** from the **Element Manager** window. The Switch Binding – State Change dialog box is displayed (Figure 71).



☑ Enable Switch Binding

Connection Policy

○ Restrict E_Ports

○ Restrict F_Ports

● Restrict All Ports

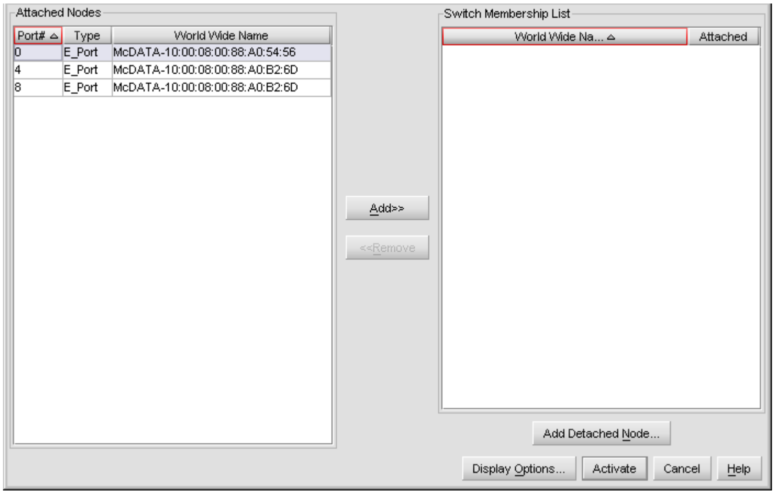
Figure 71 Switch Binding – State Change dialog box

2. Perform one of the following steps:
   - To enable Switch Binding (check mark is not in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to add a check mark. Go on to step 3 to set the Connection Policy.
   - To disable Switch Binding (a check mark is displayed in the **Enable Switch Binding** check box), click the **Enable Switch Binding** check box to remove the check mark.
3. Click one of the Connection Policy options:
   - **Restrict E_Ports**—Select if you want to restrict connections from specific switches to switch E_Ports. Switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Devices are allowed to connect to any F_Port.
   - **Restrict F_Ports**—Select if you want to restrict connections from specific devices to switch F_Ports. Device WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection. Switches are allowed to connect to any E_Port.
   - **Restrict All**—Select if you want to restrict connections from specific devices to switch F_Ports and switches to switch E_Ports. Device and switch WWNs can be added to the Switch Membership List to allow connection and removed from the Membership List to prohibit connection.
4. Click **Activate**.
5. Edit the Switch Membership List through the Switch Binding – Membership List dialog box to add or remove switches and devices that are allowed to connect with the switch.

Editing the Switch Membership List

1. Select **Configure > Switch Binding > Edit Membership List** from the **Element Manager** window. The Switch Binding – Membership List dialog box is displayed (Figure 72).

The WWNs of devices and switches that can currently connect to switch ports are listed in the Switch Membership List.



Attached Nodes

Port# △	Type	World Wide Name
0	E_Port	McDATA-10:00:08:00:88:A0:54:56
4	E_Port	McDATA-10:00:08:00:88:A0:B2:6D
8	E_Port	McDATA-10:00:08:00:88:A0:B2:6D

Switch Membership List

World Wide Na... △	Attached

Figure 72 Switch Binding – Membership List dialog box

See ""Editing the Switch Membership List" on page 120" for information on how the Switch Membership List is populated with WWNs according to options set in the Switch Binding – State Change dialog box.

2. If nicknames are configured for WWNs through HAFM and you want these to display instead of WWNs in this dialog box, click **Display Options**. The Display Options dialog box is displayed.
3. Click **Nickname**, then click **OK**.
4. To prohibit connection to a switch port from a WWN currently in the Switch Membership List, click the WWN or nickname in the Switch Membership List, then click **Remove**. The WWN or nickname moves to the Attached Nodes List. WWNs can only be removed from the fabric if any of the following is true:
   - The switch is offline.
   - Switch Binding is disabled.
   - The switch or device with the WWN is not connected to the switch.
   - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding – State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if the Switch Binding Connection Policy was enabled to `Restrict F_Ports`.
   - The switch or device with the WWN is connected to a port that is blocked.
5. The switch or device with the WWN is not currently connected to the switch (detached node).
6. WWNs can be added to the Switch Membership List (and thereby allowed connection) when Switch Binding is either enabled or disabled. To allow connection to a switch port from a WWN in the Attached Nodes List, select the WWN or nickname in the Attached Nodes List, then click **Add**. The WWN or nickname moves to the Switch Membership List.

7. To add a WWN for a device or switch not currently connected to the switch, click **Add Detached Node**. The Add Detached Node dialog box is displayed.
8. Enter the appropriate WWN or nickname (if configured through HAFM) and click **OK**. The WWN or nickname is displayed in the Switch Membership List.
9. Click **Activate**.

Enable/disable and online state functions

In order for Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Switch Binding can be enabled or disabled whether the switch is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding, Switch Binding, or both.
- If Enterprise Fabric Mode is enabled and the director or switch is offline, you can disable Switch Binding, but Enterprise Fabric Mode disables.
- WWNs can be added to the Switch Membership List when Switch Binding is enabled or disabled.
- WWNs can only be removed from the Switch Membership List if any of the following are true:
    - The director or switch is offline.
    - Switch Binding is disabled.
    - The switch or device with the WWN is not connected to the director or switch.
    - Switch Binding is not enabled for the same port type as enabled for the Connection Policy in the Switch Binding – State Change dialog box. For example, a WWN for a switch attached to an E_Port can be removed if Switch Binding Connection Policy was enabled to `Restrict F_Ports`.
    - The switch or device with the WWN is connected to a port that is blocked.
    - The switch or device with the WWN is not currently connected to the director or switch (detached node).
- If the director or switch is online and Switch Binding is not enabled, all nodes and switches attached to the director or switch are automatically added to the Switch Membership List.

Zoning with Switch Binding enabled

SANtegrity has no effect on existing zoning configurations. However, if a device WWN is in a specific zone, but the WWN is not in the Switch Membership List, the device cannot log in to the director or switch port and cannot connect to other devices in the zone with Switch Binding enabled.

Port Fencing

Port Fencing is a policy-based feature that allows the user to set thresholds on port events. If the port generates more events in a user-specified time period than you think is acceptable, Port Fencing blocks the port, disabling transmit and receive traffic until you have a chance to investigate, solve the problem, and manually unblock the port.

Access the Port Fencing Policy dialog box by selecting **Configure > Port Fencing**. The Port Fencing dialog box displays the existing policies that are discovered on HP directors and switches running firmware 07.x and later. Use this dialog to name a policy, set the limit and period and select objects to which to apply the policy. If a switch does not support Port Fencing, the ISL threshold box displays a `Port Fencing Not Supported` message.

Configuring Port Fencing

To configure port fencing, the following requirements must be met:

- To configure Port Fencing, you must have one of the following models, which must be running firmware 7.0 or later:
  - Edge Switch 2/16
  - Edge Switch 2/24
  - Edge Switch 2/32
  - Director 2/64
  - Director 2/140

Firmware 7.x supports ISL protocol fencing only. Firmware 8.x supports ISL protocol, link fencing, and security fencing. All switches must be discovered directly using MPI.

Adding thresholds

HAFM allows you to manage ISL protocol, link, and security thresholds.

Adding ISL Protocol thresholds

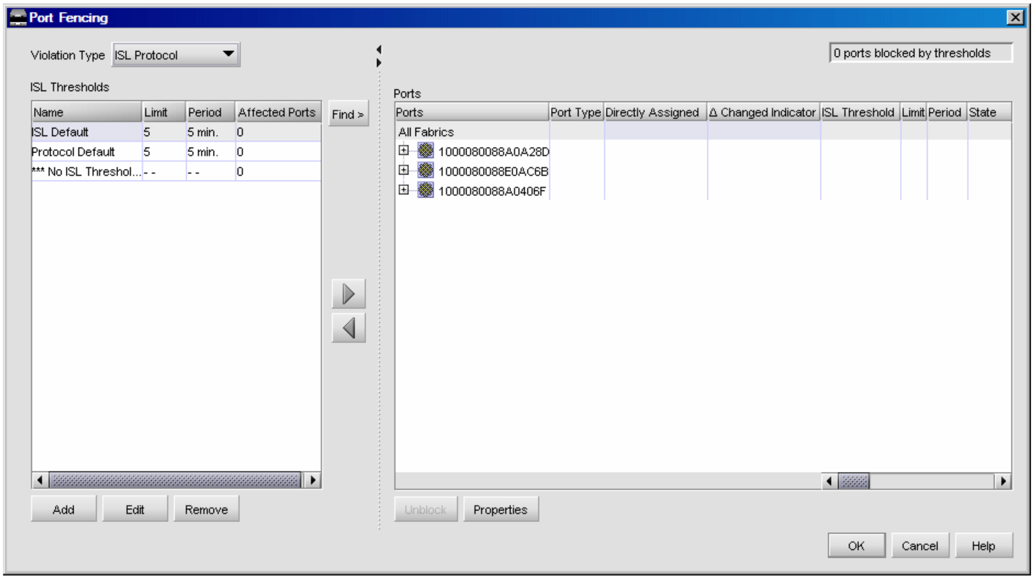
Use an ISL protocol threshold to block a port when one of the following ISL protocol errors meets the threshold:

- **ISL Bouncing**—ISL has repeatedly become unavailable due to link down events.
- **ISL Segmentation**—ISL has repeatedly become segmented.
- **ISL Protocol Mismatch**—ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

To add ISL Thresholds:

1. Select **Configure > Port Fencing**.

The Port Fencing dialog box is displayed (Figure 73).



Port Fencing

Violation Type: ISL Protocol

0 ports blocked by thresholds

ISL Thresholds

Name	Limit	Period	Affected Ports
ISL Default	5	5 min.	0
Protocol Default	5	5 min.	0
*** No ISL Threshol...	- -	- -	0

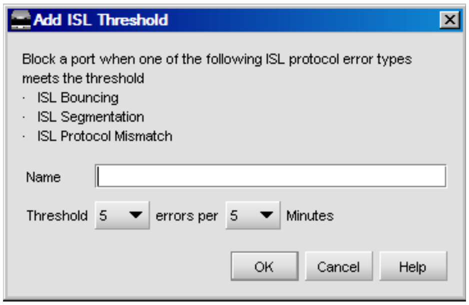
Ports

Ports	Port Type	Directly Assigned	Δ Changed Indicator	ISL Threshold	Limit	Period	State
All Fabrics							
⊞ 1000080088A0A28D							
⊞ 1000080088E0AC6B							
⊞ 1000080088A0406F							

Figure 73 Port Fencing dialog box

2. Select **ISL Protocol** from the Violation Type list.
3. Click **Add**.

   The Add ISL Threshold dialog box is displayed (Figure 74).



Add ISL Threshold

Block a port when one of the following ISL protocol error types meets the threshold

- ISL Bouncing
- ISL Segmentation
- ISL Protocol Mismatch

Name:

Threshold 5 errors per 5 Minutes

Figure 74 Add ISL Threshold dialog box

4. Enter a name for the threshold in the Name box.
5. Select the number of port events allowed for the threshold from the Threshold errors list.
6. Select the time period for the threshold from the Threshold Minutes list.
7. Click **OK** to add the ISL threshold to the table and close the Add ISL Threshold dialog box.
8. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
9. Click **OK**.

Adding link thresholds

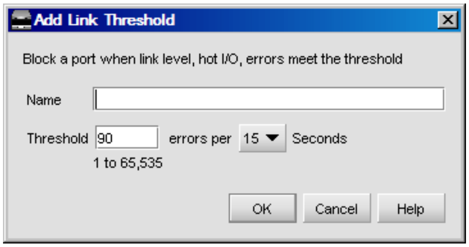
Use the link threshold to block a port when a Link Level (Hot I/O) error meets the threshold. Active Loop ports repeatedly received LIP and active non-loop ports repeatedly received LR, OLS or NOS.

To add a Link Threshold:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select **Link** from the Violation Type list.
3. Click **Add**.

   The Add Link Threshold dialog box is displayed (Figure 75).



Add Link Threshold

Block a port when link level, hot I/O, errors meet the threshold

Name

Threshold 90 errors per 15 Seconds

1 to 65,535

Figure 75 Add Link Threshold dialog box

4. Enter a name for the threshold in the Name box.
5. Select the number of port events allowed for the threshold from the Threshold errors list.
6. Select the time period for the threshold from the Threshold Seconds list.
7. Click **OK** to add the Link threshold to the table and close the Add Link Threshold dialog box.
8. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
9. Click **OK**.

Adding security thresholds

Use the security threshold to block a port when one of the following security violations occurs:

- **Authentication**—The switch is unavailable due to Authentication events.
- **Fabric Binding**—The switch is unavailable due to Fabric Binding events.
- **Switch Binding**—The switch is unavailable due to Switch Binding events.
- **Port Binding**—The switch is unavailable due to Port Binding events.
- **ISL Security (Generic Security Error)**—The switch on the other side of the ISL detected a specific security violation, but only indicates that a generic security violation has occurred or a security configuration mismatch was detected.
- **N_Port Connection Not Allowed**—The switch is unavailable due to N_port connection not allowed events.

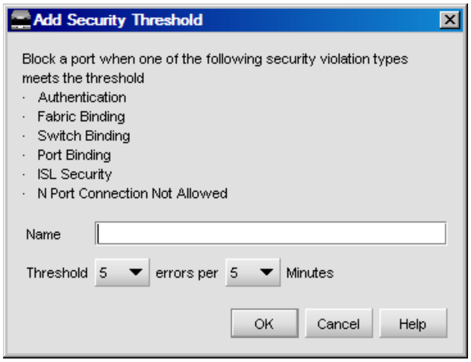
To add Security Thresholds:

1. Select **Configure > Port Fencing**.

The Port Fencing dialog box is displayed (Figure 73 on page 124).

2. Select **Security** from the Violation Type list.
3. Click **Add**.

   The Add Security Threshold dialog box is displayed (Figure 75).



Block a port when one of the following security violation types meets the threshold

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name

Threshold 5 errors per 5 Minutes

Figure 76 Add Security Threshold dialog box

4. Enter a name for the threshold in the Name box.
5. Select the number of port events allowed for the threshold from the Threshold errors list.
6. Select the time period for the threshold from the Threshold Seconds list.
7. Click **OK** to add the security threshold to the table and close the Add Security Threshold dialog box.
8. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
9. Click **OK**.

Assigning thresholds

To assign thresholds:?

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select a threshold type from the Violation Type list.
3. Select the threshold you want to assign in the ISL Thresholds table.
4. Select the objects (All Fabrics, Fabric, Switch, Port Type (Security only), and/or Port) to which you want to assign the threshold in the Ports table.
5. Click ▷ to assign the threshold.

   An icon displays next to the objects you selected in the Ports table to show that the threshold was applied at this level and was inherited by each object below it in the tree (if not affected by lower level direct assignments).

   An icon displays next to each object in the tree to which the new threshold is applied.
6. Click **OK**.

Editing thresholds

HAFM allows you to edit the name, number of events, and time period of ISL protocol, link, and security thresholds.

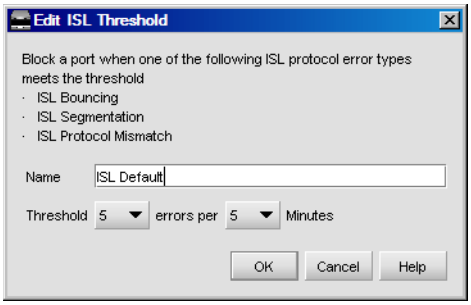
Editing ISL Protocol Thresholds

To edit an ISL protocol threshold:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select **ISL Protocol** from the Violation Type list.
3. Click **Edit**.

   The Edit ISL Threshold dialog box is displayed (Figure 77).



Edit ISL Threshold

Block a port when one of the following ISL protocol error types meets the threshold
- ISL Bouncing
- ISL Segmentation
- ISL Protocol Mismatch

Name: ISL Default

Threshold: 5 errors per 5 Minutes

Figure 77 Edit ISL Threshold dialog box

4. Make changes to the threshold, if necessary.
5. Click **OK** to accept the changes and close the Edit ISL Threshold dialog box.

   If the threshold has already been assigned to ports, the message `This edit will apply to affected switches` is displayed. Click **OK** to close.
6. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
7. Click **OK**.

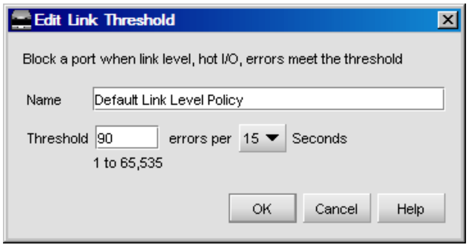
Editing link thresholds

To edit a link threshold:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select **Link** from the Violation Type list.
3. Click **Edit**.

The Edit Link Threshold dialog box is displayed (Figure 78).



Block a port when link level, hot I/O, errors meet the threshold

Name: Default Link Level Policy

Threshold: 90 errors per 15 Seconds

1 to 65,535

Figure 78 Edit Link Threshold dialog box

4. Make changes to the threshold, if necessary.
5. Click **OK** to accept the changes and close the Edit Link Threshold dialog box.

   If the threshold has already been assigned to ports, the message `This edit will apply to affected switches` is displayed. Click **OK** to close.
6. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
7. Click **OK**.

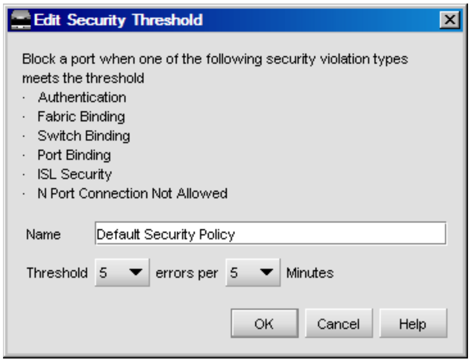
Editing security thresholds

To edit a security threshold:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select **Security** from the Violation Type list.
3. Click **Edit**.

   The Edit Security Threshold dialog box is displayed (Figure 79).



Block a port when one of the following security violation types meets the threshold

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name: Default Security Policy

Threshold: 5 errors per 5 Minutes

Figure 79 Edit Security Threshold dialog box

4. Make changes to the threshold, if necessary.
5. Click **OK** to accept the changes and close the Edit Security Threshold dialog box.

   If the threshold has already been assigned to ports, the message `This edit will apply to affected switches` is displayed. Click **OK** to close.

6. To assign this threshold to fabrics, switches, or switch ports, see "Assigning thresholds" on page 126.
7. Click **OK**.

Finding assigned thresholds

HAFM allows you to find all ports with a specific threshold applied.

To find assigned thresholds:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select a threshold type from the Violation Type list.
3. Select a threshold from the Threshold table.
4. Click **Find**.

   Each port that uses the selected threshold is highlighted in the Ports table.
5. Click **OK**.

Viewing thresholds

To view thresholds:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select a threshold type from the Violation Type list.
3. Review the Thresholds and Ports tables.
4. Click **OK**.

Removing thresholds

When you assign a new threshold to an object, the old threshold is automatically removed. HAFM also allows you to remove thresholds from an individual fabric, switch, or switch port, from all fabrics, switches, and switch ports at once, as well as from the Threshold table.

To remove thresholds from all Fabrics, Switches, and Switch Port s, as well as the Threshold table:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).
2. Select a threshold type from the Violation Type list.
3. Select the object with the threshold you want to remove from the Ports table.
4. Click ◀ to remove the threshold.

   A icon is displayed next to every instance where the threshold was removed from an object, if there was another threshold higher in the tree that is now inherited by the object.

   A icon is displayed next to the affected objects.

To remove thresholds from all Fabrics, Switches, and Switch Ports, as well as the Threshold table:

1. Select **Configure > Port Fencing**.

   The Port Fencing dialog box is displayed (Figure 73 on page 124).

2. Select a threshold type from the Violation Type list.
3. Select the threshold you want to remove from the Thresholds table.
4. Click **Remove**.

   If this threshold is assigned to a fabric, switch, or switch port, a message is displayed, asking if you want to delete this threshold from its assigned ports. Click **OK** to continue.

   A icon is displayed next to each instance where the threshold was removed from an object, if there was another threshold higher in the tree that is now inherited by the object.

   A icon is displayed next to the each affected object and does not inherit a threshold from higher in the tree.
5. Click **OK**.

Open trunking

Open trunking is an optional license-keyed feature that monitors the data flows on ISLs (from a receive port to a target domain) and periodically reroutes data from congested links to lightly loaded links. It makes the most efficient use of redundant ISLs between switches.

Load balancing does not require user configuration, other than to enable open trunking. However, you can modify default settings for congestion thresholds (per port).

You do not need to manually configure ISLs into *trunk groups* of redundant links where data can be off-loaded. Open trunking identifies candidate links for rerouting and maintains the links automatically.

Options

Access open trunking through the HAFM menu bar. Figure 80 shows the Configure Open Trunking dialog box. Table 18 describes the function of each option.

Table 18 Open trunking configuration options

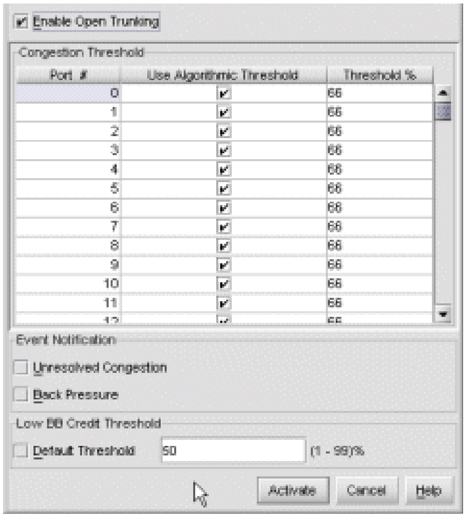
Option	Function (when enabled)
Enable Open Trunking	Enables the open trunking option
Congestion Thresholds	Sets the congestion threshold levels for ports as percentages (1%—99%) of link bandwidths. When the link's traffic load becomes *congested*, traffic is rerouted (if possible) to an uncongested link. Two options are available: • Select the check box under the Use Algorithmic Threshold column to use a value computed by the rerouting algorithm. • Click in the Threshold **%** column, and enter a value in the range of 1 through 99.
Event Notification	Identifies the type of events that result in an event log entry, and generates an SNMP trap. The notifications occur on first instance only. The event notification types are: • Unresolved congestion—The rerouting algorithm cannot find a path for rerouting data flow to relieve congestion. • Back Pressure—The low BB_credit threshold has been exceeded.
Low BB_Credit threshold	Defines the acceptable percent of time that the transmitting link has no BB_credit. Two options are available: • Default threshold value • User-defined threshold value

Configuration

To enable open trunking for a switch and configure threshold values and event notification options:

1. Select **Configure > Open Trunking**.

The Configure Open Trunking dialog box is displayed (Figure 80).



☑ Enable Open Trunking

Congestion Threshold

Port #	Use Algorithmic Threshold	Threshold %
0	☑	66
1	☑	66
2	☑	66
3	☑	66
4	☑	66
5	☑	66
6	☑	66
7	☑	66
8	☑	66
9	☑	66
10	☑	66
11	☑	66
12	☑	66

Event Notification

□ Unresolved Congestion

□ Back Pressure

Low BB Credit Threshold

□ Default Threshold 50 (1 - 99)%

Figure 80 Configure Open Trunking dialog box

2. Select the **Enable Open Trunking** check box.
3. Specify the congestion threshold value.

   If you do not specify a threshold value for a port, open trunking uses a default value that is based on port type (1 Gb/s or 2 Gb/s) and channel bandwidth.
4. Select the Event Notification options, as appropriate.
5. Set the low BB Credit threshold value.
6. Click **Activate**.

Global threshold changes

In the Configure Open Trunking dialog box, right-click a column in the Configuration Threshold table to display menu options that globally change values.

- **Use Algorithmic Threshold**—Right-click this column to display these options:
  - **Set All to Default**—Adds check marks to all check boxes in this column and sets all cells of Threshold % column to default values
  - **Clear All**—Clears all check boxes in this column and restores values in cells of Threshold % column with previous values
- **Threshold %**—Right-click this column to display these options:
  - **Set All To xx**—Sets all cells in this column to the value (xx) that you clicked
  - **Restore All**—Sets all cells in the column to the previous values

Open Trunking log

The Open Trunking log (Figure 81) provides details on flow rerouting through switch ports.

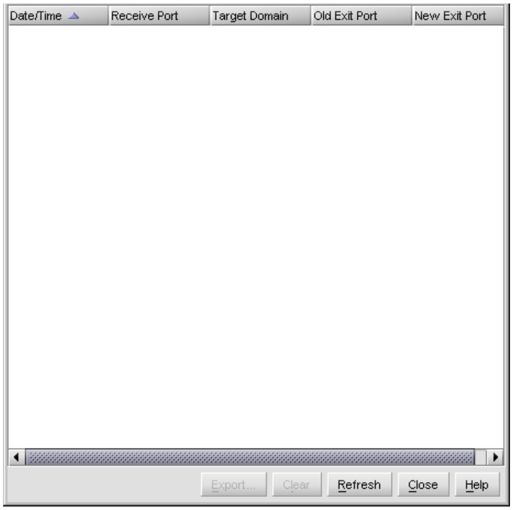


Figure 81 Open Trunking log

The log lists the following:

- **Date/Time**—The date and time of the rerouting occurrence
- **Receive Port**—The receive port number (decimal) on the local switch associated with the flow that was rerouted
- **Target Domain**—The domain ID (decimal) associated with the flow that was rerouted
- **Old Exit Port**—The exit port number (decimal) on this switch that the flow used to access the target domain
- **New Exit Port**—The exit port number (decimal) on this switch that the flow now uses to access the target domain

Performance Module

Performance Module is a feature that you use to monitor SAN devices. For information about event monitoring and notification, see the HAFM online help.

Displaying connection utilization

The HAFM application shows the percentage of data utilization of the trunks.

To display the connection utilization legend:

Select **Monitor Utilization > On** from the main window menu bar (or press **Ctrl-U**).

To turn utilization off:

Select **Monitor > Utilization > Off** from the main window menu bar.

See "Viewing the HAFM main window" on page 33 for details.

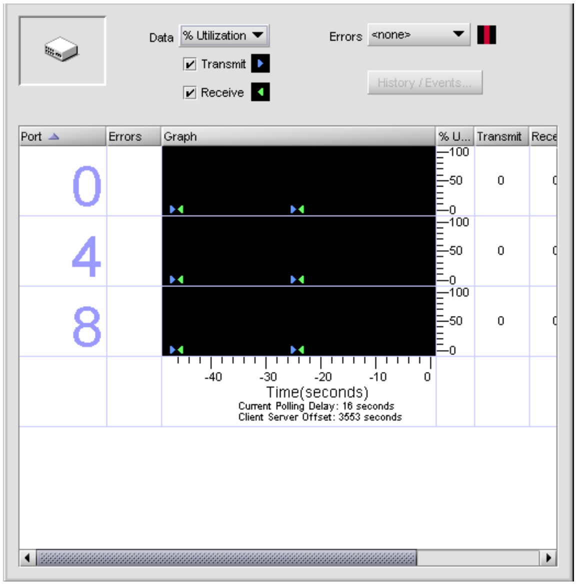
Monitoring switch performance

A performance graph shows transmit, receive, and error data from the switch ports to the connected devices. The graphs can be sorted by the errors, transmit data, or receive data.

To monitor switch performance:

1. Right-click a switch icon on the HAFM Physical Map and select **Performance Graphs**.

   The Performance Graph dialog box is displayed (Figure 82).



Data % Utilization

☑ Transmit

☑ Receive

Errors <none>

Figure 82 Performance graph dialog box

2. Select the type of data to display from the Data list.
3. Select the error data to display from the Errors list.

Collecting performance data

You can collect performance data about your SAN and then view it or export it and distribute the data to others.

Storing performance data

To store SAN performance data, select **Monitor > Performance > Store Data**.

Viewing performance data

See the HAFM online help for instructions on how to generate and view HTML reports of performance data.

Exporting performance data

To export SAN performance data to communicate issues to the support center, capture network status, and archive historical data, see "Exporting and importing data" on page 51 or see the HAFM online help.

NOTE: Currently, you can export only to the same versions of the application.

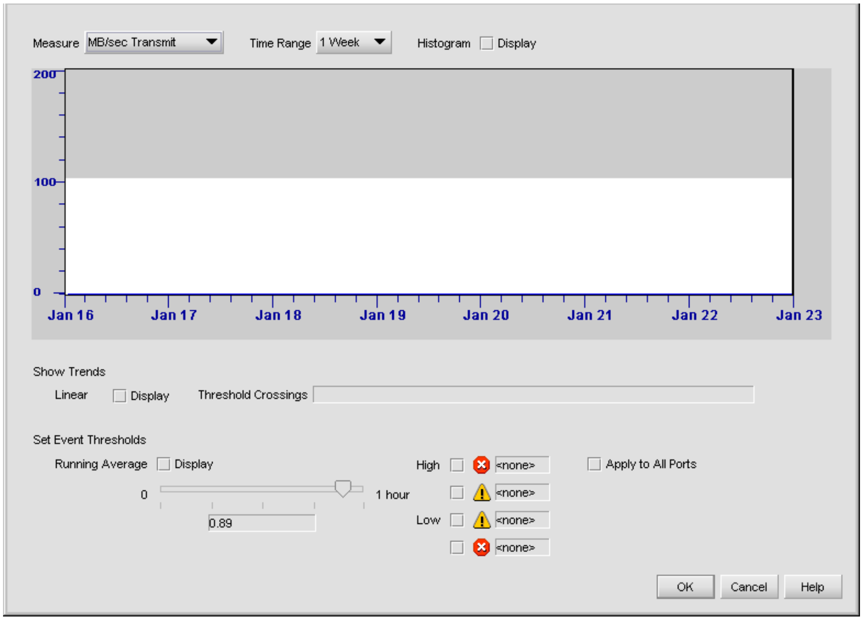
Monitoring port performance

You can monitor the performance of switch ports devices in the SAN using the port performance graph. The graph also shows information about transmit and receive performance.

To monitor port performance:

1. Right-click a switch icon on the Physical Map and select **Performance Graphs**.

   The Performance Graph dialog box is displayed (Figure 82).
2. Select a port row and click **History/Events** (or double-click a port row) to display the Port Performance Graph dialog box (Figure 83).



Measure: MB/sec Transmit
Time Range: 1 Week
Histogram □ Display

Show Trends
Linear □ Display
Threshold Crossings

Set Event Thresholds
Running Average □ Display
0 — 1 hour
0.89
High □ <none>
□ <none>
Low □ <none>
□ <none>
□ Apply to All Ports

Figure 83 Port Performance Graph dialog box

3. Select options from the following lists to customize the performance graph:

- **Measure**—Assigns a unit of measure for the graph.
- **Time Range**—Selects a time range.

- **Histogram Display**—Shows the percentage of trunk utilization over a period of time.

  Move the Histogram slide bar to change the period of time displayed.
- **Linear Display**—Shows a linear average of the trunk utilization. This function provides a forward-looking trend analysis and is intended to notify the user of resource modeling problems.
- **Running Average Display**—Applies an averaging algorithm to the display. This display can be adjusted on a varying percentage of an hour. To change the display, move the slide bar.

4. Select the check boxes next to ✖ and ⚠ to define the boundaries to configure both high and low usage performance warnings and critical thresholds.
5. Adjust the slide bars at the right side of the display.

   As you move a slide bar, the percentage of utilization is displayed in the associated box.
6. Set separate transmit and receive thresholds in either %Utilization or MB/sec. Set separate error thresholds.

   If **Running Average Display** is selected, your thresholds are triggered only if the running average crosses the threshold.
7. Click **Apply to All Ports** if you want to apply your changes to all ports on the device.
8. Click **OK**.

NOTE: Port performance data and thresholds are indexed by node name. If you move a switch from one location to another, it brings its performance data and thresholds with it. Additionally, if a threshold is set in one SAN file and the same port is discovered in a different SAN file, the threshold is defined in both files.

Planning Module

The Planning Module enables you to plan and evaluate a SAN before you implement the design. You can use a discovered SAN as the basis for a plan, eliminating the need to duplicate a design.

Planning window

The Planning window (Figure 84) differs slightly from the window that shows a discovered SAN. The Planning window has:

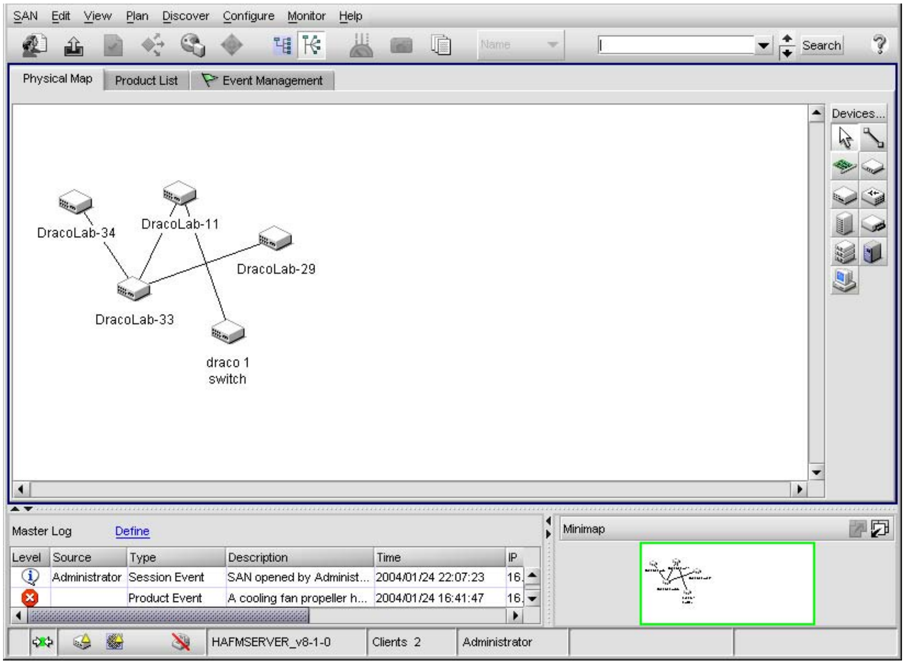
- Three tabs:
  - Physical Map
  - Product List
  - Event Management
- A menu bar

  Click a menu item to see a list of available options.
- A device toolbox

  The toolbox provides tools to add, select, and connect devices in the SAN. To see a definition of a tool, position your curser over the tool.
- Master log

- Minimap

Select **View > Planned SAN**. The Planning window is displayed (Figure 84).



Level	Source	Type	Description	Time	IP
ⓘ	Administrator	Session Event	SAN opened by Administ...	2004/01/24 22:07:23	16.
☒		Product Event	A cooling fan propeller h...	2004/01/24 16:41:47	16.

Figure 84 Planning window

Plan design

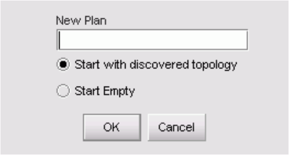
By designing a plan, you can configure, connect, and arrange planned devices. This saves you cost and time by enabling you to evaluate the plan before implementing the design.

Planning a SAN

To plan a new SAN:

1. Select **SAN > New Plan** (or press **Ctrl-N**) from the Planning window menu.

   The New Plan dialog box is displayed (Figure 85).



New Plan

● Start with discovered topology

○ Start Empty

Figure 85 New Plan dialog box

2. Enter a name in the New Plan box.

3. Select one of the following options:
   - **Start with discovered topology**—Use the discovered topology as the basis for the new plan.
   - **Start Empty**—Start the new plan with an empty topology.
4. Click **OK**.

Opening a plan

To open a plan:

1. Select **SAN > Open Plan** from the Planning window menu (or press **Ctrl-O**).

   The Open Plan dialog box is displayed (Figure 86).

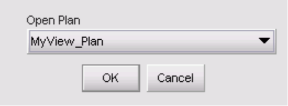

Open Plan: MyView_Plan

Figure 86 Open Plan dialog box

2. Select a plan from the Open Plan list.
3. Click **OK**.

Adding devices

You can add one device or multiple devices to the plan.

Adding one device

To add one device:

1. Click a device icon on the devices toolbox.
2. Click the Physical Map in the Planning window.

   The new planned device icon is displayed on the Physical Map.

Adding multiple devices

To add multiple devices:

1. Click the devices icon on the devices toolbox.

   The Insert Multiple Devices dialog box is displayed (Figure 87).

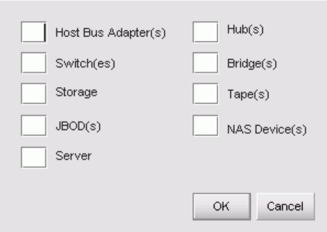


Figure 87 Insert Multiple Devices dialog box

2. Enter a quantity for each device type you want to add.
3. Click **OK**.

Arranging devices

After adding devices to your plan, you can rearrange them

To rearrange a device:

1. Click the **Select Devices** icon ( ) on the devices toolbox.
2. Click a planned device icon and drag it to the desired location.
3. Repeat as necessary.

Connecting devices

To connect the devices:

1. Click the **Connect Devices** icon ( ) on the devices toolbox.
2. Click a device on the Physical Map.

   A connection is created and associated with the first available port on the device.
3. Click another device on the Physical Map.

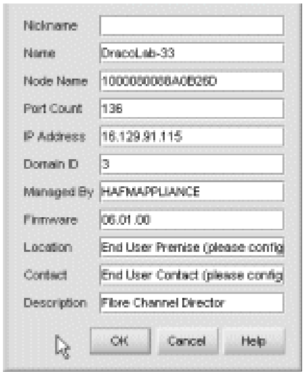
   The connection is associated with the first available port on the second device. A connection is displayed between the two devices.
4. If you want to make multiple connections, click the **Connect Devices** icon ( ), hold down the **Shift** key, and click each device you want to connect.

Configuring devices

To specify properties for planned devices:

1. Right-click a planned device icon on the Physical Map and select **Properties**.

   The planned device's Properties dialog box is displayed (Figure 88).



Nickname

Name DracoLab-33

Node Name 1000080088A0B26D

Port Count 136

IP Address 16.129.91.115

Domain ID 3

Managed By HAFMAPPLIANCE

Firmware 06.01.00

Location End User Premise (please config

Contact End User Contact (please config

Description Fibre Channel Director

Figure 88 Planned device Properties dialog box

2. Enter a nickname for the device in the Nickname box (optional).
3. Enter or edit information.
4. Click **OK**.

Deleting devices

To delete planned devices, right-click the planned device icon on the Physical Map and select **Delete**.

Displaying a planned device as an installed device

Right-click a planned device icon on the Physical map and select **Planned Device**.

- If the **Planned Device** option is selected, the device icon is displayed inside a box icon.
- If the option is not selected, the device icon is displayed without a box.

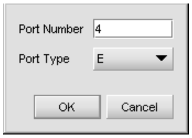
Editing port types

To arrange devices and edit a planned device's port types:

NOTE: You can perform this task only in the Planning window.

1. Select **View > Planned SAN** from the Planning window menu.
2. Add devices as necessary.
3. Rearrange devices as necessary.
4. Connect the devices.
5. Right-click a planned device icon and select Ports to view the device's ports.
6. Click the black arrow next to the port number.

   The Port Properties dialog box is displayed (Figure 89).



Port Number 4

Port Type E

Figure 89 Port Properties dialog box

7. Enter a port number in the Port Number box.
8. Select a port type from the Port Type list (available only for multiport devices).
9. Click **OK**.
10. Optionally, right-click a planned device icon and select **Planned Device**.

    The device changes from a planned device to an implemented device.

Configuring ports

You can configure port numbers and types for planned devices.

NOTE: To configure planned ports, planned devices must be connected.

1. Right-click a planned device icon on the Physical Map and select **Ports**.

2. Click the small triangle next to the port number.

   The Port Properties dialog box is displayed (Figure 89).
3. Enter a number in the Port Number box.
4. Select a port type from the Port Type list.
5. Click **OK**.

Planning rules

This section describes how to use planning rules to evaluate a plan.

Planning rules specify criteria for a plan evaluation. Rules are stored in the text file `Install_Home\Server\Config\Other\rules.dat`. You can open the `rules.dat` file using any text editor.

Planning rules syntax and format

Planning rules must follow a certain syntax and format. Table 19 describes the planning rule parameters.

NOTE: You must be an advanced user with administrator privileges to edit planning rules.

The following example shows the syntax for a planning rule:

```
set rule_id = SAN_1
where rule = “check_for_valid IPAddress for (device=switch or device=hub or
device=bridge)”
and description = “valid IP addresses must be specified for all switches,
hubs and bridges”
and headline = “Valid IP must be specified/property validation”
and errormssg = “The device labeled {0} has invalid IP address”
and remedy = “Please specify a valid IP address”;
```

Table 19 Planning rule parameters

Parameter	Required to load rule?	Description	Format
set rule_id	Yes	Sets the rule ID.	Must be a unique value, but can be any length and format.
where rule	Yes	Sets the actual rule. A list of rule types follows this table.	Use only the keywords provided; otherwise the rule fails.
description	No	Provides a more detailed description of the rule.	Must be prepended with an "and." Must be enclosed within quotation marks.
headline	No	Provides a short overview of the rule.	Must be prepended with an "and." Must be enclosed within quotation marks.
errormsg	No	Specifies the error message to display if the rule is violated. If this statement is not specified, or if it is null, a generic error message is displayed.	Must be prepended with an "and." Must be enclosed within quotation marks.
remedy	No	Specifies a remedy for the rule violation. This text is displayed on the evaluation window.	Must be prepended with an "and." Must be enclosed within quotation marks.

Rule types

There are three types of rules that define the `where rule` parameter:

- **Connection rules**—Specify which devices can be connected in a plan (Table 20).
- **Property validation rules**—Verify the validity or uniqueness of device names in a plan (Table 21).
- **Capacity control rules**—Verify the connections in a plan Table 22).

Keywords

NOTE: Keywords are not case sensitive.

The `where rule` parameter allows the following keywords:

- Types:
    - Device
    - Network
    - Zone
    - Fabric
    - Switch, Hub, Bridge, NAS, HBA, Storage, Tape, JBOD, Loop, Server
- Property names:
    - Wwn
    - Portwwn
    - Model
    - IPAddress
    - SerialNumber
    - Vendor
    - Firmware
    - PortType
    - PortNumber
    - ZoneName
    - F_Port, FL_Port, TL_Port, E_Port, NL_Port, N_Port, H_Port, UNKNOWN_PORTs
    - MAXPORTS

- Operators: =, <, <=, >, >=

Table 20 Connection rules

Syntax	Description
do_not_connect (device=x)	Never connect device x to device x.
do_not_connect (device=x) to (device=y)	Never connect device x to y.
do_not_connect (device=x) to (device=y) through (device=z)	Never connect device x to y through z.
do_not_attach (device=x) to (device=y)	Never connect device x into a SAN that has device y.
connect (device=x)	Always connect device x to device x.
connect (device=x) to (device=y)	Always connect device x to y.
connect (device=x) to (device=y) through (device=z)	Always connect device x to y through z.

Table 21 Property validation rules

Syntax	Description
check_for_valid '*PropertyName*' for (device=x)	Device *x* must have valid 'PropertyName'.
'*PropertyName*' should_be_unique_in '*Types*'	Cannot have duplicate 'PropertyName' in the same 'Types'.

Table 22 Capacity control rules

Syntax	Description
total_connections (device = *x*) '*Operator*' 2	The sum of connections to device *x* should be 'Operator' than 2total_connections.
(device = *x*) '*Operator*' MAXPORTS	The sum of connections to device *x* should be 'Operator' than MAXPORTS.
total_connections (device = *x*) to (device = *y*) '*Operator*' 2	The sum of connections from device *x* to device *y* should be 'Operator' than 2.

Applying rules for plan evaluation

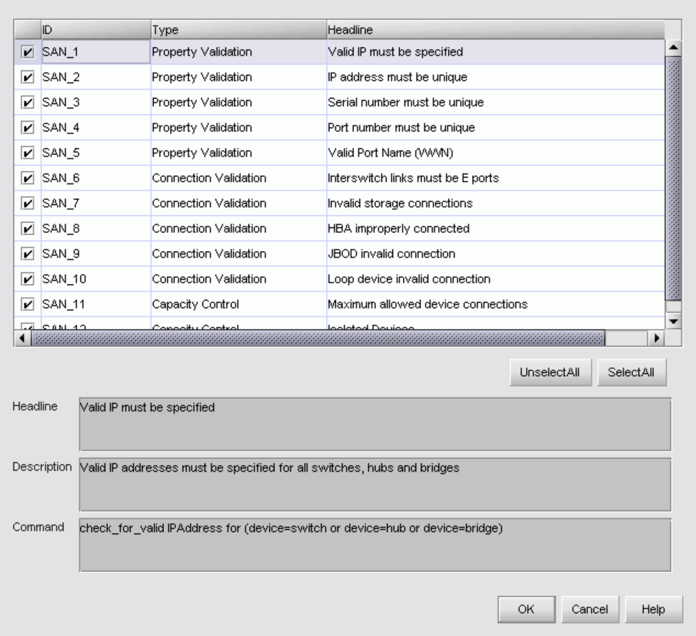
To apply rules for evaluating the plan:

1. Select **View > Planned SAN.**

   The Planning window is displayed (Figure 84).

2. Select **Plan > Set Rules** from the Planning window menu bar.

   The Planning Rules dialog box is displayed (Figure 90.)



	ID	Type	Headline
☑	SAN_1	Property Validation	Valid IP must be specified
☑	SAN_2	Property Validation	IP address must be unique
☑	SAN_3	Property Validation	Serial number must be unique
☑	SAN_4	Property Validation	Port number must be unique
☑	SAN_5	Property Validation	Valid Port Name (WWN)
☑	SAN_6	Connection Validation	Interswitch links must be E ports
☑	SAN_7	Connection Validation	Invalid storage connections
☑	SAN_8	Connection Validation	HBA improperly connected
☑	SAN_9	Connection Validation	JBOD invalid connection
☑	SAN_10	Connection Validation	Loop device invalid connection
☑	SAN_11	Capacity Control	Maximum allowed device connections
☑	SAN_12	Capacity Control	Isolated Devices

Headline: Valid IP must be specified

Description: Valid IP addresses must be specified for all switches, hubs and bridges

Command: check_for_valid IPAddress for (device=switch or device=hub or device=bridge)

Figure 90 Planning Rules dialog box

NOTE: If spelling or syntax errors are detected, the rule cannot display in the Planning Rules dialog box.

3. Select the rules you want to apply when evaluating the plan.
4. Click **OK**.

Plan evaluation

To evaluate a plan:

1. Select **SAN > Open plan** from the Planning window menu bar to open the plan.
2. Select **Plan > Evaluate**.

   The application evaluates the plan and shows the results in the SAN Evaluation Report window.
3. Review the report. Click the hyperlinks to jump to devices and view the tips to determine resolutions.
4. Resolve the issues.
5. Select **Plan > Evaluate** to revaluate the plan.
6. Repeat step 2 through step 5 if more problems are identified.

Plan conservation

This section describes how to save, export, and print a plan.

Saving a plan

After you design a plan, you can save it for future reference.

To save a plan with its current name, select **SAN > Save Plan** from the planning window menu. The plan is saved with the current name.

To save a plan with a new name:

1. Select **SAN > Save as Plan** from the Planning window menu bar**.**

   The Save As dialog box is displayed.
2. Enter a new file name in the Save As box.
3. Click **OK**.

Exporting a plan

You can export planning files to share your plan with others or to archive it for future reference.

Follow the instructions described in "Exporting data" on page 52.

Printing a plan

You can export a plan as a Physical Map in JPG format. You can then print the JPG file from a photo application or a web browser.

7 Zoning

Zoning defines the communication paths in a fabric. A zone consists of initiator and target ports in the SAN. Ports can communicate only with other ports in their zone. However, ports can be members of more than one zone. To zone devices in a fabric, the fabric's principal switch must be an HP switch and HAFM must discover and manage it.

HAFM performs zoning discovery once at startup, and thereafter once every two hours during routine discovery. For best results, HP recommends that you perform zoning five discovery cycles after starting the HAFM appliance.

The following zoning features are described:

- Zoning limits, page 147
- Zoning naming conventions, page 148
- Zoning configuration, page 148
- Zoning administration, page 156

Zoning limits

You can configure large zone sets with HAFM. Table 23 lists the zoning limits for the edge switches and directors.

NOTE: Hard zoning is enforced when the firmware initializes. Devices not conforming to zoning rules are restricted to their assigned zones.

Table 23 Zoning parameter limits

Zoning parameter	Maximum value
Number of zone members in a zone	2048
Number of zones in a zone set[1]	1024
Number of unique zone members in a zone set	2048
Total number of zone members in a zone set (where a zone member can be in multiple zones)	4096
Characters per zoning name	32
Number of unique zone members in HAFM zoning library	2048
Number of zones in HAFM zoning library	1024

Table 23 Zoning parameter limits (continued)

Zoning parameter	Maximum value
Number of zone sets in HAFM zoning library	64
Number of end ports	1024
Number of devices supported (including loop devices)	1024

[1] The supported number of zones is based on a zone name with a maximum of 32 characters. On all edge switches and directors (except the Director 2/140), the maximum number of zones decreases if the names are 64 characters long. The limits are based on two members per zone.

Zone set sizes are determined by the:

- Number of zones in the zone set
- Length of each zone name
- Number of members in each zone
- Interoperability mode of the fabric

Contact HP Professional Services or your support representative if you have questions regarding specific zone set configurations.

Zoning naming conventions

The following rules apply for zone names and zone set names:

- Names must begin with alphabetic characters, but can include alphanumeric characters and underscores.
- Names must be unique and are case insensitive.
- Names cannot include spaces.
- Names cannot begin with `SANav_` because it is reserved.
- Names can have a maximum of 57 characters.
- No duplicate names are allowed in zones, zone sets, or zone libraries.

Zoning configuration

Use the Zoning dialog box (Figure 91) to configure zoning. When the Zoning dialog box is open, zoning discovery is performed during every polling cycle for up to 30 minutes, after which it is performed once every two hours.

You can:

- Display the zone library (see "Displaying the zone library" on page 149).
- Create and add a zone to a zone set (see "Adding a zone to a zone set" on page 150).
- Create and add members to a zone (see "Adding a member to a zone" on page 150).
- Create a zone set (see "Creating a zone set" on page 151).

- Remove a member from a zone (see "Removing a member from a zone" on page 152).
- Remove a zone from a zone set (see "Removing a zone from a zone set" on page 152).
- Activate a zone set (see "Activating a zone set" on page 152).
- Deactivate a zone set (see "Deactivating a zone set" on page 153).
- Enable or disable the default zone (see "Enabling and disabling the default zone" on page 154).
- Export a zone set (see "Exporting a zone set" on page 155).
- Import a zone set (see "Importing a zone set" on page 156).

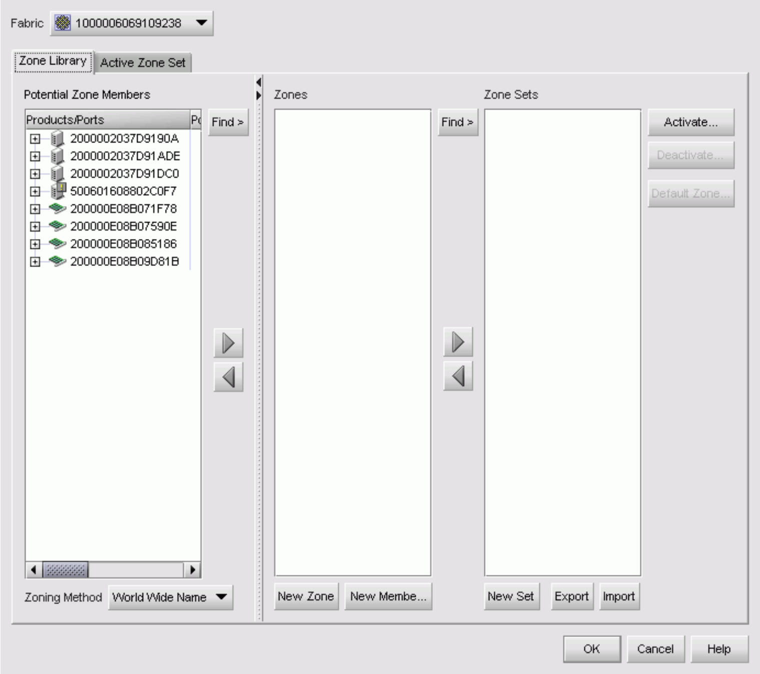
NOTE: Only one appliance should perform discovery at a time, otherwise logon conflicts can occur.

Displaying the zone library

To display the zone library:

1. Select **Configure > Zoning**.

   The Zoning dialog box is displayed (Figure 91).



Fabric 1000006069109238

Zoning Method World Wide Name

Figure 91 Zoning dialog box

2. Select a fabric from the Fabric list.

   This defines the fabric for the zoning actions.

3. Click the Zone Library tab.

   The Zones, Zone Sets, and Potential Zone Members lists are displayed.

NOTE: If the Zoning dialog box is open for longer than 30 minutes, the information displayed cannot be current. Reopen the dialog box to increase zoning discovery speed and get the updated information.

Adding a zone to a zone set

To add a new or existing zone to a zone sets:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. To create a new zone, click **New Zone**.

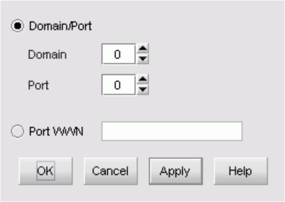
   A new zone is displayed in the Zones list.
3. To add an existing zone, proceed to step 9.
4. Rename the zone. See "Zoning naming conventions" on page 148.
5. Select the members to add to the new zone from the Potential Zone Members list.
6. Select the new zone from the Zones list.
7. Click ▶ to the right of the Potential Zone Members list to add the selected members to the zone.
8. Select an option from the Zoning Method list.
9. Select the zone sets to which you want to add the zone from the Zone Sets list.
10. Select the zones you want to add to the zone set from the Zones list.
11. Click ▶ to the right of the Zones list to add the selected zones to the zone sets.
12. To activate the zone set, see "Activating a zone set" on page 152.
13. Click **OK**.

Adding a member to a zone

To add a new or existing member to a zone:

1. Display the zone library. See "Displaying the zone library" on page 149.
2. Select the zones to which you want to add members from the Zones list.
3. To add an existing member, skip to step 7.
4. To create a new member, click **New Member**.

The Add Zone Member dialog box is displayed (Figure 92).



● Domain/Port

Domain: 0

Port: 0

○ Port WWN

Figure 92 Add Zone Member dialog box

5. Specify a zone member by its domain and port ID or WWN address.

NOTE: Zoning by domain and port is supported only in Homogeneous Fabric interop mode.

Do one of the following:

- Select **Domain/Port** and enter the domain and port IDs in the appropriate boxes.
- Select **WWN** and enter the WWN address.

NOTE: If you select an invalid domain/port value or WWN address and then activate the zone set, the application shows a zoning mismatch message after the next discovery pass.

6. Click **OK**.

   The Zoning dialog box is displayed (Figure 91 on page 149).
7. Select an option from the Zoning Method list.
8. Select the members to add to the zone from the Potential Zone Members list. To add all ports on a device, select the device.
9. Click ▷ to the right of the Potential Zone Members list to add the selected members to the zone.
10. Click **OK**.

NOTE: If you click **Cancel** or the close button (X), without clicking **OK**, only the changes that you made to the active zone set are saved.

Creating a zone set

To create a new zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Click **New Set** to create a new zone set.
3. Rename the zone set. See "Zoning naming conventions" on page 148.
4. Press **Enter**.

5. Select the zones you want to add to the zone set from the Zones list.
6. Click ▶ to the right of the Zones list to add the selected zones to the zone set.
7. To activate the zone set, see "Activating a zone set" on page 152.
8. Click **OK**.

Removing a member from a zone

1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Expand a zone by clicking the + symbol in the Zones list.
3. Right-click the member you want to remove and click **Remove**.
4. Click **OK**.

Removing a zone from a zone set

1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Expand a zone set by clicking the + symbol in the Zone Sets list.
3. Right-click the zone you want to remove and click **Remove**.
4. Click **OK**.

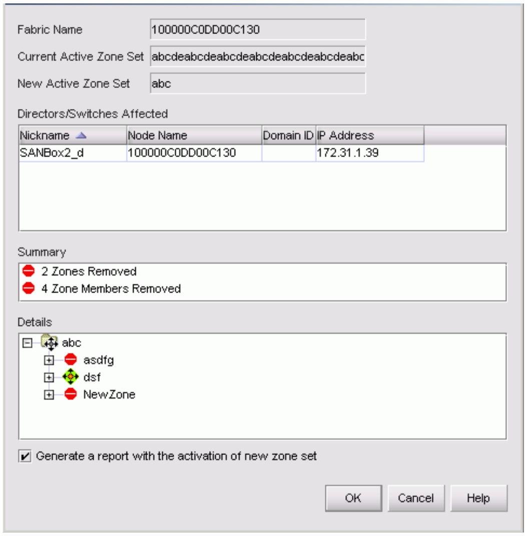
Activating a zone set

NOTE: Activation speeds can vary depending on the hardware vendor and type of zoning used.

To activate a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select a zone set from the Zone Sets list.
3. Click **Activate**.

The Activate Zone Set dialog box is displayed (Figure 93).



Fabric Name: 100000C0DD00C130

Current Active Zone Set: abcdeabcdeabcdeabcdeabcdeabcdeabc

New Active Zone Set: abc

Directors/Switches Affected

Nickname	Node Name	Domain ID	IP Address
SANBox2_d	100000C0DD00C130		172.31.1.39

Summary

2 Zones Removed

4 Zone Members Removed

Details

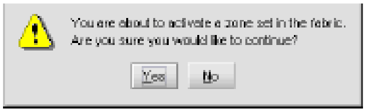
abc
- asdfg
- dsf
- NewZone

☑ Generate a report with the activation of new zone set

Figure 93 Activate Zone Set dialog box

4. Verify the information and click **OK**.

   A confirmation message is displayed (Figure 94).



You are about to activate a zone set in the fabric.
Are you sure you would like to continue?

Figure 94 Activate Zone Set confirmation message

5. Click **Yes** to continue.

   The Zoning dialog box is displayed.

6. Click the **Active Zone Set** tab to view the active zone set and its zones.

   Verify that the switch is being managed properly.

NOTE: Only one appliance should perform discovery at a time; otherwise, logon conflicts can occur.

7. Click **OK**.

Deactivating a zone set

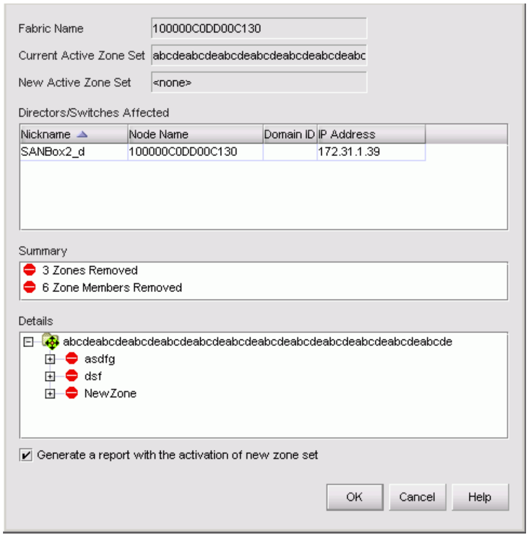
To deactivate a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).

2. Click **Deactivate**.

The Deactivate Zone Set dialog box is displayed (Figure 95).



Fabric Name 100000C0DD00C130

Current Active Zone Set abcdeabcdeabcdeabcdeabcdeabcdeabc

New Active Zone Set <none>

Directors/Switches Affected

Nickname	Node Name	Domain ID	IP Address
SANBox2_d	100000C0DD00C130		172.31.1.39

Summary

3 Zones Removed

6 Zone Members Removed

Details

abcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcdeabcde
- asdfg
- dsf
- NewZone

☑ Generate a report with the activation of new zone set

Figure 95 Deactivate Zone Set dialog box

The dialog box shows the names of the active zone set, and shows the new active zone set as `none`. Verify the information in this dialog box.

3. Click **OK**.

   The active zone set and its zones are deactivated.

NOTE: If the default zone is enabled and the active zone set is deactivated, members of the zone can still be able to communicate.

Enabling and disabling the default zone

By enabling the default zone, the potential zone members that are not in zones can see all other potential members that are not in zones.

To enable the default zone:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select the fabric for which you want to enable the default zone.
3. Enable the default zone by selecting **Default Zone**.
4. Click **OK**.

NOTE: Default zones are only supported in Homogeneous Fabric interop mode. Default zones are not supported in Open Fabric interop mode. If default zoning is not available, the Default Zone button is disabled.

To disable the default zone:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select the fabric for which you want to disable the default zone.
3. Disable the default zone by selecting **Default Zone**.
4. Click **OK**.

Exporting a zone set

You can export a zone set as an XML file and import it to a different zone set library on the HAFM appliance or to a zone set library on another appliance.

NOTE: You can export only one zone set at a time.

To export a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select the zone set that you want to export in the Zone Sets list.
3. Click **Export**.

   The Export Zone Set dialog box is displayed (Figure 96).

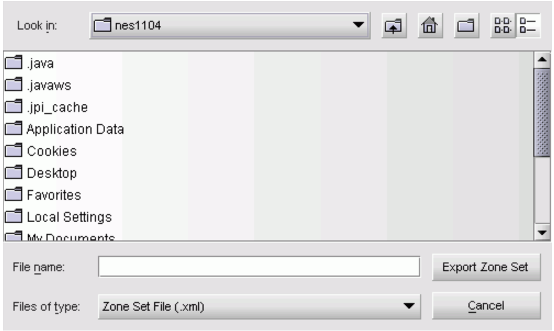


Figure 96 Export Zone Set dialog box

4. Select the folder in which you want to save the XML file.
5. Enter a name for the file in the File name box.

6. Click **Export Zone Set**.

   The file is saved to the specified folder.

7. Click **OK**.

Importing a zone set

To import a zone set XML file to a zone set library:

1. Display the zone library. (See "Displaying the zone library" on page 149.)

   The Zoning dialog box is displayed (Figure 91 on page 149).

2. Click **Import**.

   The Import Zone Set dialog box is displayed (Figure 97).

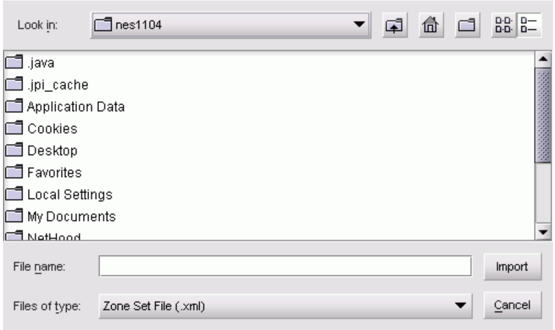


Figure 97 Import Zone Set dialog box

3. Locate the folder that contains the exported zone set.
4. Select the XML file and click **Import**.

NOTE: If the zone set name already exists in the zone set library, a warning message is displayed: `Unable to import zoneset. The zoneset name already exists.` Change the zone set name and try again.

5. Click **OK**.

Zoning administration

This section describes zoning administrative tasks. Tasks that you can perform on zones and zone sets include:

- Renaming a zone or zone set, page 157
- Replacing zone members, page 157
- Copying a zone set, page 158
- Deleting a zone, page 158
- Viewing zone and zone set properties, page 159
- Finding members in a zone, page 159

- Finding zones in a zone set, page 159
- Displaying zone members, page 159
- Saving the active zone set to a zoning library, page 160
- Comparing zone sets, page 160

Renaming a zone or zone set

To rename a zone or zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Right-click the zone or zone set that you want to rename and select **Rename**.
3. Enter the new name. See "Zoning naming conventions" on page 148.
4. Press **Enter** to save the new name.

Replacing zone members

You can replace zone members in one of two ways:

- Select the replacement zone member from the Potential Zone Member list.
- Specify the replacement member's domain/port or WWN.

Using the Potential Zone Members list

To replace a zone member:

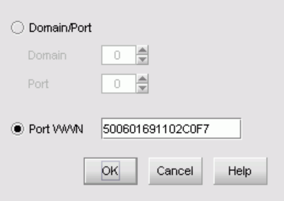
1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select the member you want to replace from the Potential Zone Members list.
3. Click **Find** to find all instances of the member in the configured zones.
4. Click ◀ to the right of the Potential Zone Members list to remove the member from the zones.
5. Select the replacement member from the Potential Zone Members list.
6. Click ▶ to the right of the Potential Zone Members list to add the member to the zones.
7. Click **OK**.

Using the domain/port or WWN

To replace a zone member:

1. Display the zone library. See "Displaying the zone library" on page 149.
   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Right-click the member you want to replace and select **Replace**, or right-click in the Zones area and select **Replace All**.

The Replace Zone Member dialog box is displayed (Figure 98).



○ Domain/Port

Domain 0

Port 0

● Port WWN 500601691102C0F7

Figure 98 Replace Zone Member dialog box

3. Enter the domain and port IDs or the WWN of the replacement member.
4. Click **OK**.

Copying a zone set

To copy a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91).
2. Right-click the zone set that you want to copy.
   - Select **Duplicate** to copy the zone set.
   - Select **Deep Duplicate** to copy the zone set and its zones.

   The copied zone set is displayed.
3. Optionally, enter a new name for the zone set. See "Replacing zone members" on page 157.
4. Click **OK**.

Deleting a zone

To delete a zone:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Right-click the zone you want to delete and click **Delete**.

NOTE: The zone is deleted without confirmation. If you delete a zone accidentally, click **Cancel** instead of **OK** to restore it.

3. Click **OK**.

Deleting a zone set

To delete a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Right-click the zone set you want to delete and click **Delete**.

NOTE: The zone set is deleted without confirmation. If you delete a zone set accidentally, click **Cancel** instead of **OK** to restore it.

3. Click **OK**.

Viewing zone and zone set properties

You can view information for zones and zone sets, such as names; number of zones, zone sets, or zone members; number of unique zone members; and status.

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Right-click a zone or zone set and select **Properties**.
3. Click **Close** when you have finished viewing the properties.

Finding members in a zone

To find members in a zone:

1. Display the zone library. See"Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select a device or port from the Potential Zone Members list and click **Find**.

   All found members are highlighted in the Zones list.

Finding zones in a zone set

To find members in a zone set:

1. Display the zone library. See "Displaying the zone library" on page 149.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select a zone from the Zones list and click **Find**.

   All zones found are highlighted in the Zone Sets list.

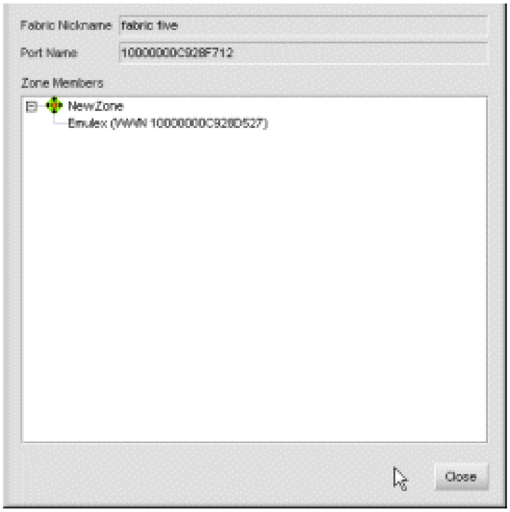
Displaying zone members

To display zone members:

1. Select **View All > Levels > All Levels**.

   All levels are displayed on the Product List.
2. Expand a product on the Product List to display the ports.
3. Right-click a port and select **List Zone Members.**

The List Zone Members dialog box is displayed (Figure 99).



Fabric Nickname: fabric five

Port Name: 10000000C928F712

Zone Members

- NewZone
  - Emulex (WWN 10000000C928D527)

Figure 99 List Zone Members dialog box

4. Click **Close** to close the dialog box.

Saving the active zone set to a zoning library

When you manage a switch's zone set through one appliance, and then import that switch to a new appliance, you must save the zone set on the new appliance, This allows preexisting zoning information on the switch to be stored on the new appliance.

To save the active zone set to a zoning library:

1. Select **Configure > Zoning**.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select a fabric from the Fabric list.
3. Click the **Active Zone Set** tab.
4. Select the active zone set and click **Save As**.

   The Save Active Zone Set As dialog box is displayed.
5. Rename the active zone set and click **OK**.

   The switch's zoning information is imported to the new appliance. You can now manage zones and zone sets through the new appliance.

Comparing zone sets

To compare two zone sets:

1. Select **Configure > Zoning**.

   The Zoning dialog box is displayed (Figure 91 on page 149).
2. Select a fabric from the Fabric list.
3. Click the **Activate Zone Set** tab.

4. Click **Compare With**.

   The Select a Zone Set dialog box is displayed.

5. Select a zone set and click **OK**.

   The comparison results are displayed.

8 SANtegrity Security Center

This chapter provides instructions for using the SANtegrity Security Center.

Security Center Overview

The Security Center is a tool for viewing and configuring your installation's Fibre Channel authentication parameters. The Security Center provides a single central user interface for managing the authentication settings of all SANtegrity-capable switches and directors in the installation. The SANtegrity Security Center includes:

- The list of fabrics.
- Summaries of the security configuration for each SANtegrity-capable device in each fabric.
- Configuration tabs for updating each switch's SANtegrity authentication values. The tabs are each oriented around a specific authentication task. For example, there is a tab to define which users are allowed to sign on to the switch to perform management tasks, and which management interfaces are enabled; and there is a tab to define the IP addresses from which management requests can originate, and whether the switch or director will limit management requests based on originating IP address.
- The ability to easily apply changes to all switches or directors in a fabric. This key feature allows you to define the authentication parameters for one switch, and, by a few simple additional clicks, propagate the changes to one or more additional switches in the fabric. Thus, the Security Administrator can view and manage security settings for entire fabrics at once.
- A Security Log containing a record of all security-related configuration updates, as well as security-related events such as illegal login requests.

The Security Center is designed to be a single point of control for the Security Administrator. Although the Element Manager has the ability to configure the SANtegrity parameters for a single switch, only the Security Center provides installation-wide Fibre Channel security configuration and monitoring.

Accessing the Security Center

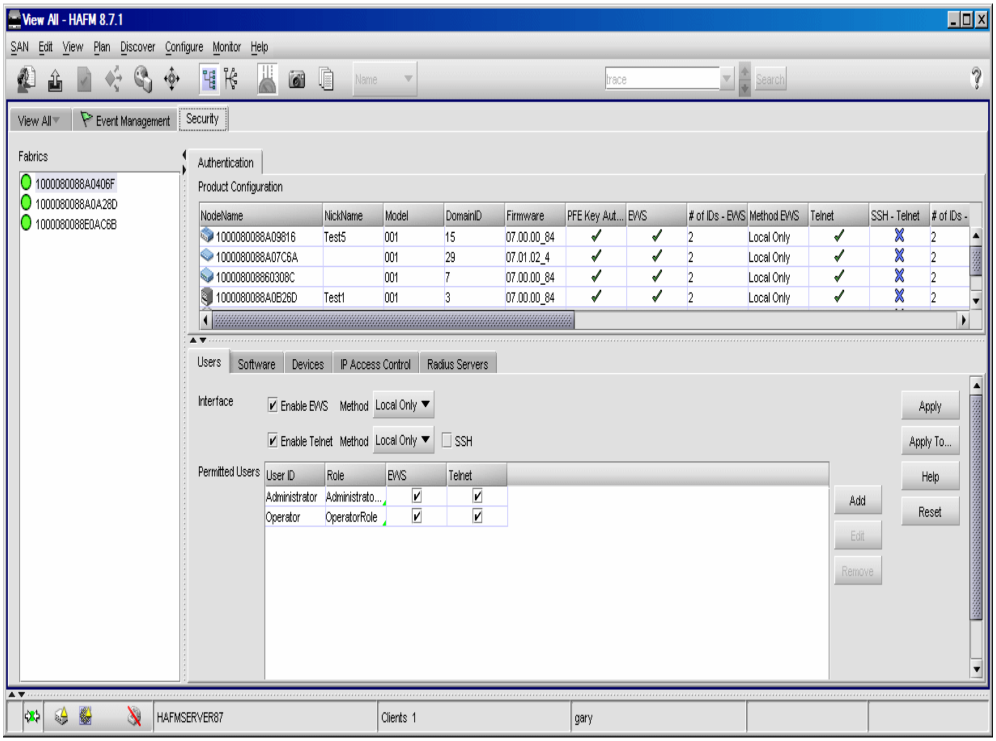
The SANtegrity Security Center feature requires a license key, and is not available unless the Security license key is installed on the HAFM appliance. The SANtegrity Security Center is accessed from the Security tab on the main window and displays fabric information, authentication information, Master Log, and Security Log.

Access the SANtegrity Security Center by clicking the **Security** tab or pressing **F8** on the main window. In order to use the Security Center, the user must have Security Administrator privilege. If not, the Security tab is hidden.

Additional information about the components of the Security window follows:

- The upper left part of the Security window shows the Fabrics list. All discovered fabrics are listed by their WWNs with their operational status icons on the left side.
- The upper right part of the Security window displays the main working area, where the Security Administrator configures the authentication security settings. The main working area is divided into two parts:
  - The upper part is the Authentication Product Configuration table, which contains a summary of security-related values for each switch in a fabric.
  - The lower part is a tabbed pane containing a set of five tabs for completing security configuration tasks.
- The lower left part of the Security window displays the server Master Log; the lower right part of the window displays the Security Log.
- The Security tab and Security Log are only available to users with Security Administrator privileges.
- Change the default size of the display by placing the cursor on the divider until a double arrow is displayed. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.
- On the toolbar, the Display By option and the Search Box option are disabled.

NOTE: SANtegrity Authentication can also be accessed from any SANtegrity-capable Element Manager by selecting **Configure > SANtegrity Authentication**. Accessing SANtegrity Authentication from the Element Manager allows you to manage only one device at a time.



NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

Interface ☑ Enable EWS Method Local Only

☑ Enable Telnet Method Local Only ☐ SSH

Permitted Users

User ID	Role	EWS	Telnet
Administrator	Administrato...	☑	☑
Operator	OperatorRole	☑	☑

Figure 100 Security Center

Displaying the Fabrics list

The Fabrics list displays all discovered fabrics listed by their WWNs with their operational status on the left side if the status is available. When a fabric is selected from the left side, all switches within the fabric are displayed in the top table. This includes devices not managed by this HAFM appliance and offline devices.

Although all devices display, only HP products managed by the HAFM appliance can be configured. These products display with their corresponding product icon. These are the same icons shown on the topology map.

If an HP product is not managed by the HAFM appliance, the product displays a generic icon. If the product is offline, a customized product icon is displayed with a unknown operations status icon.

NOTE: If a device is managed by the HAFM appliance, when the device displayed on the Security tab is offline or loses a MPI link, the previously discovered value can still display in the top table. If this switch is selected, a blank area is displayed in the bottom pane with an error message.

Using the Authentication table

The Authentication table includes summary data about each switch or director in a fabric. This includes security and nonsecurity information. This table automatically refreshes to reflect the latest changes to the products listed. Some information is not available for switches and directors that are not managed or that are not at the correct firmware level.

Selecting a fabric

When a fabric is selected from the left side, all switches within the fabric are displayed on the top table of the Authentication table. Note the following specifics:

- Only HP products that are currently being managed by the HAFM appliance can be configured. These products are represented by their corresponding customized product icons on the topology map. These are the only products whose security settings can be discovered and displayed.
- A generic icon is displayed for all products that are not managed by the HAFM appliance.
- If a switch goes offline, then the switch does not display in the top table and a warning message indicates there are unapplied changes on the tab. If you click off the tab, all the changes are lost for that tab.
- An offline switch is contained in its own fabric and works like a managed switch. The icon for the offline switch is the customized product icon.
- If none of the discovered products is manageable when the Security tab is first accessed, a message is displayed indicating this device cannot be configured because it is not currently managed by this HAFM appliance.
- If you select a switch and start to configure the settings, and then the switch goes offline or loses the MPI link, you can continue configuring the switch by clicking **Yes** in the displayed warning message. You can apply all changes to the offline switch and all changes are populated to the switch. Alternatively, you can wait until the switch is online and the changes made to the top table can be applied.
- If the switch is manageable and you complete the configuration changes from the bottom tabs and apply them to the Authentication table, and then the switch loses manageability before you click **Activate**, a message indicates that you cannot apply the changes because the switch is not manageable. However, you can apply the changes when the switch is manageable again, as long as you do not exit the window.

Changing security data internally

The Authentication table automatically refreshes to reflect the latest changes to the products listed. The changes include security-related or nonsecurity data. With nonsecurity data, the table refreshes and regular events are generated for the changes and logged in the Master Log.

Changing security data externally

When security data is changed by another interface such as HTTP or Telnet, the Security Administrator should be notified because the working data can be affected by the table's live update.

If the security settings for a switch or director are changed by another management interface, then the following occurs:

- If the switch that was changed by another interface is not currently configured by your HAFM appliance user, the top table accepts the changes, and an event is generated in the Security Log.
- If the changes made by another interface affect the switch whose security data is currently being modified by a Security Administrator, a message is displayed indicating the security settings have been changed by an external source. The message asks you if you want to load the new settings from the switch or keep your changes.
  - Click **Load New Settings**—The information is displayed on the top table and configuration on the bottom tab update. All working data is overridden by the new data in the switch.
  - Click **Keep Changes**—The updates are made to the switch, but you can maintain the configuration both on the top table and bottom tab. If needed, these changes can be overridden with the current configuration.

Accessing SANtegrity Security Center tabs

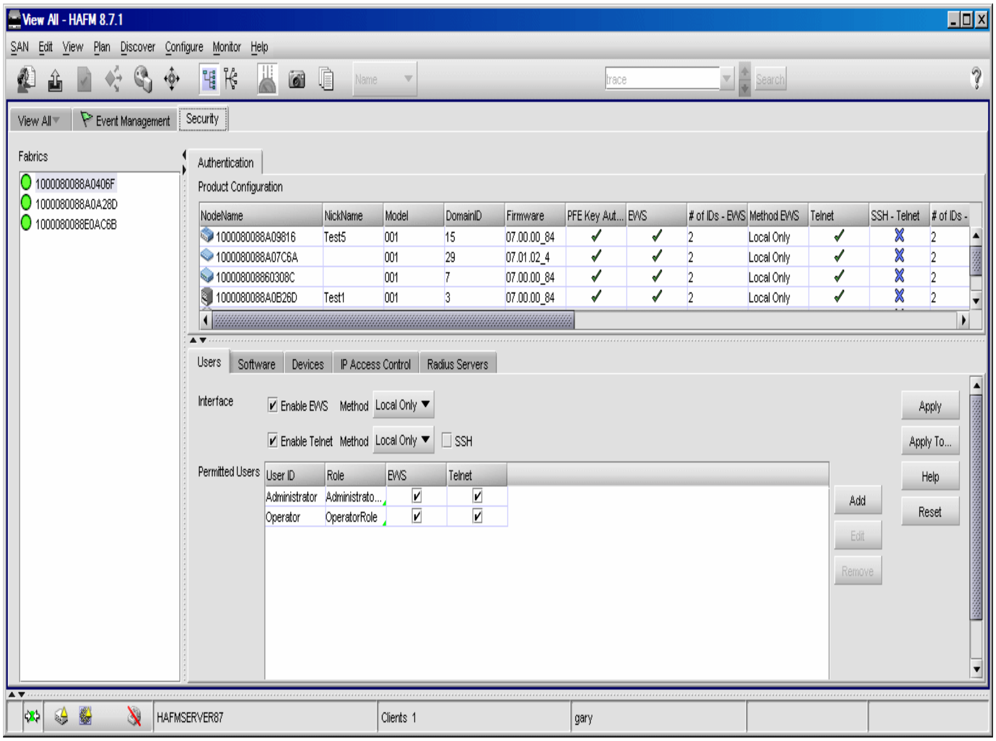
The Authentication section has five tabs:

- **Users**—Allows the Security Administrator to set up users accessing the switch from CLI and web interfaces tab, the Security Administrator specifies whether the Telnet and HAFM Basic interfaces are enabled, which method the switch or director uses to authenticate users, and which users are authorized to use these interfaces.
- **Software**—Allows the Security Administrator to set up software applications that can communicate with the switch through API.
- **Device**—Allows the Security Administrator to set device-to-device authentication parameters. The Device tab is PFE key-enabled. If a proper PFE key is not provided, the Device tab is not accessible.
- **IP Access Control**—Allows the Security Administrator to set up IP addresses to manage the switch.
- **Radius Server**—Allows the Security Administrator to set RADIUS server parameters that the switch can use to pass authentication information to the designated RADIUS servers.

The following buttons are used on the Authentication tabs:

Using the Users tab

The Security Administrator uses the Users tab to set up role-based user access to the selected switch through other management interfaces, such as HAFM Basic or Telnet.



Fabrics

1000080088A0406F
1000080088A0A28D
1000080088E0AC6B

Product Configuration

NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

Interface ☑ Enable EWS Method Local Only

☑ Enable Telnet Method Local Only ☐ SSH

Permitted Users

User ID	Role	EWS	Telnet
Administrator	Administrato...	☑	☑
Operator	OperatorRole	☑	☑

Figure 101 Security Center Users tab

If the Enable EWS (HAFM Basic) or Enable Telnet check box is not selected, then no user can log in to the switch through this interface. When the interfaces are enabled, HAFM Basic and Telnet can be set to authenticate to a local database on the switch, a RADIUS server, or a local database and then a RADIUS server. If the SSH check box is selected then all management data between the workstation and the switch through Telnet is encrypted using the SSH protocol.

If **Radius Only** is selected from the list, your HAFM appliance checks the RADIUS information to determine if a RADIUS server has been specified. If not, the application prevents the user from selecting this option and a message is displayed.

If the RADIUS server is already set, the Security Administrator is alerted that the user information on the RADIUS server must be entered manually. The HAFM appliance cannot populate that information automatically.

Assigning users to a switch

For the user role, there are two options available from a list, Administrator and Operator. The ID of the user is `Administrator` and the password is `password`. The third and fourth column indicate whether a user has access to the switch through the HAFM Basic or Telnet interface, or through both of them.

A default user is set up in the switch user base. The ID of the user is Administrator and the password is password. There is one default user displayed in the table, and the Telnet and HAFM Basic check boxes are selected.

Adding a new user

To add a new user:

1. Click **Add**.

   The Add/Edit User dialog box is displayed (Figure 102).

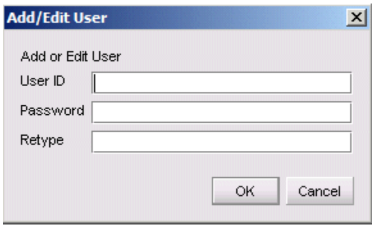


Figure 102 Add/Edit User dialog box

2. Enter information in the boxes.

   User ID must be unique. If you specify an existing ID, it will be rejected. The maximum length of password is 24 characters.
3. Click **OK**.
4. Assign the Administrator or Operator role to the user.

   By default, all new users are set up with an Administrator privileges. You can changed this by clicking the list under the Role column and selecting another option.

The Security Administrator can delete users from the switch user database. There must be at least one user with Administrator privileges for Telnet and HAFM Basic. A message is displayed if you try to delete the last user with Administrator privileges.

If a user is removed from the table, the user cannot access the switch through the Telnet or HAFM Basic interface. The removed user who is in a session with the switch can continue working on the switch until logging out.

Adding a set of users to multiple switches

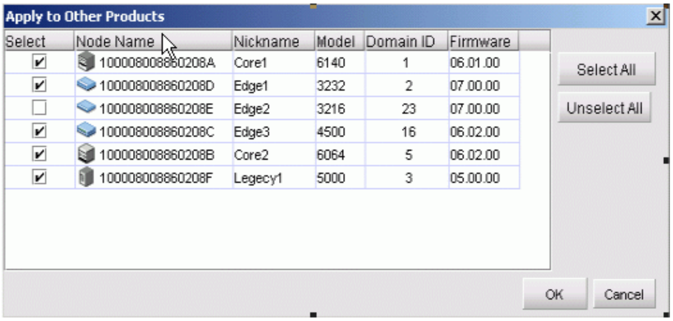
The Security Administrator can add the same set of users to multiple switches.

NOTE: This feature is not available from the Element Managers.

To add the same set of users to multiple switches:

1. Click **Apply To**.

The Apply to Other Products dialog box is displayed (Figure 103).



Apply to Other Products

Select	Node Name	Nickname	Model	Domain ID	Firmware
☑	100008008860208A	Core1	6140	1	06.01.00
☑	100008008860208D	Edge1	3232	2	07.00.00
☐	100008008860208E	Edge2	3216	23	07.00.00
☑	100008008860208C	Edge3	4500	16	06.02.00
☑	100008008860208B	Core2	6064	5	06.02.00
☑	100008008860208F	Legecy1	5000	3	05.00.00

Figure 103 Apply to Other Products dialog box

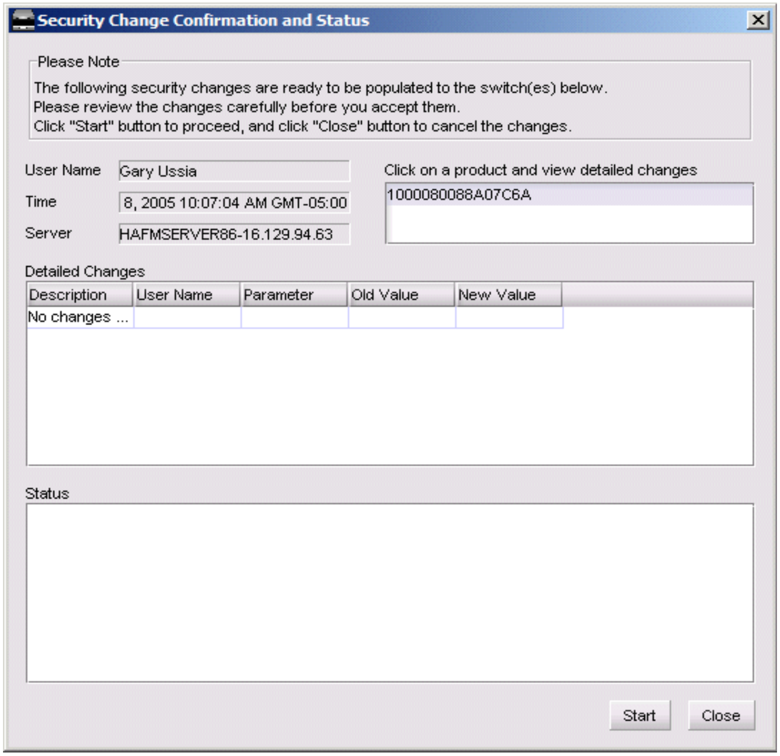
To be listed in this dialog box:

- The switches and directors must be manageable.
- The Element Manager must manage one of the following models:
    - A 16-port 1 Gb or 2 Gb switch
    - A 24-port 2 Gb switch
    - A 32-port 1 Gb or 2 Gb switch
    - A 64-port or 140-port director
- The firmware must be 7.0 or later.

2. Select the check boxes for the devices to which you want to apply the users.
3. Click **OK**.

Using the Security Change Confirmation and Status dialog box

Clicking **OK** on the Apply to Other Products dialog box or click **Apply** on the Users tab, displays the Security Change Confirmation and Status dialog box (Figure 104). This is a status-monitoring dialog box that lets you know if the changes were successful.



Security Change Confirmation and Status

Please Note

The following security changes are ready to be populated to the switch(es) below.
Please review the changes carefully before you accept them.
Click "Start" button to proceed, and click "Close" button to cancel the changes.

User Name: Gary Ussia

Time: 8, 2005 10:07:04 AM GMT-05:00

Server: HAFMSERVER86-16.129.94.63

Click on a product and view detailed changes

1000080088A07C6A

Detailed Changes

Description	User Name	Parameter	Old Value	New Value
No changes ...				

Status

Figure 104 Security Change Confirmation and Status dialog box

The Security Change Confirmation and Status dialog box lists the ID of the user ID who initiated the changes, the time that the changes were scheduled, the ID of the server from which the changes are populated, and the affected switches and directors. The server ID is the server name plus the IP address.

The Detailed Changes table lists all configurations that the Security Administrator made on the Users tab. The columns of this table vary depending on which tab the Security Administrator is accessing the confirmation information.

If there is only one product to which changes must be applied, only that product is listed. The product ID is its node name. By default, this product is highlighted.

If you applied the same user settings to multiple products, the Product List displays the product names that were selected in the Apply To dialog box. By default, the product that was selected from the top table for configuration is highlighted. The content of the Detailed Changes table changes as you scroll through products in the Product List.

The differences between the to-be-populated settings and current settings on each individual product are displayed, because the Apply To dialog box takes changes made on user settings for one product, and generalizes them to multiple products whose user settings can be totally different. The new settings replace the existing settings on other products.

To thoroughly check the new changes, click different products on the Product List and view detailed changes.

NOTE: Populating user-related settings to multiple products causes the new settings to override the existing settings.

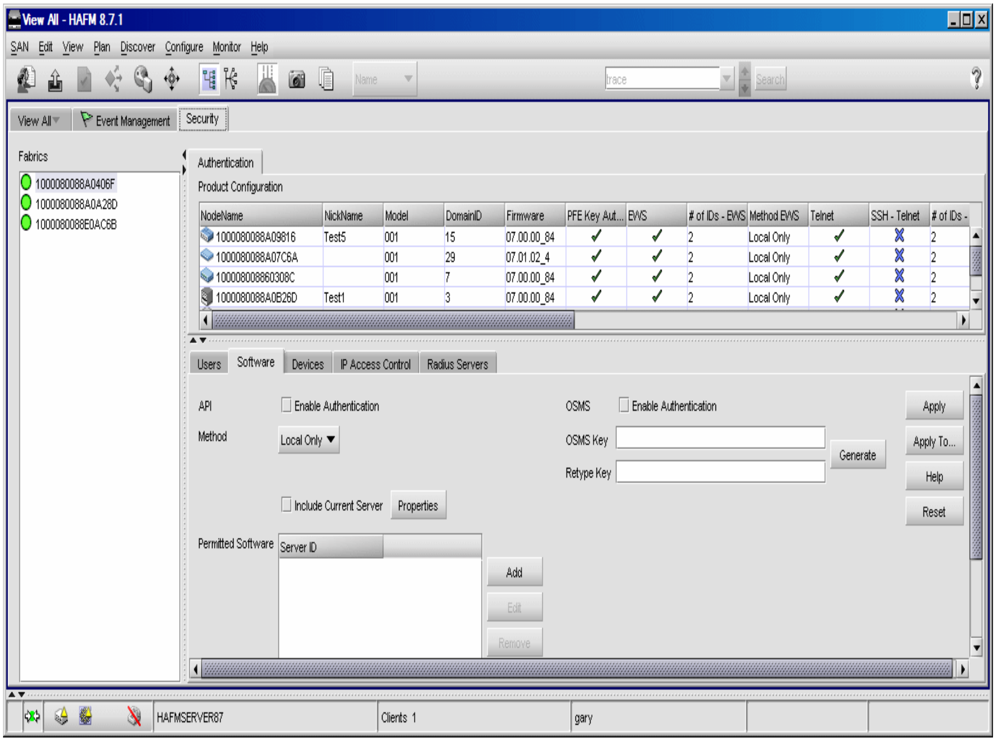
Clicking **Start** causes the HAFM appliance to populate changes to the switch specified in the products list. The Close button is disabled during this process to prevent you from disrupting the process. Close is enabled after the process is complete or the process is aborted because of a product failure.

The bottom Status window displays the status of each product. If all changes are successfully populated to a product, the status displays the product name and a message indicating success. If the switch loses manageability or connection, a message is displayed with an Error icon. The remaining changes continue to process. The Security Administrator can maintain the configuration data on the Users tab, fix the connection problems, and return to the either Apply or Apply To dialog box. Select the unfinished products and repeat the confirmation process.

If there are no security settings being changed, **Apply** and **Apply To** can be selected. When this occurs, the Security Change Confirmation and Status dialog box is displayed with the Detailed Changes table and a message indicates that no changes were found. Clicking **Start** displays a Status message that indicates the security settings are identical and that there are no changes to apply.

Using the Software tab

The Software tab (Figure 105) enables you to define software access to the switch through the API and the OSMS interface. Unlike the Telnet and HAFM Basic interfaces, the API user uses the HAFM appliance name (which is the server name defined at installation) as the ID, and uses the CHAP Secret as the password. The OSMS interface allows HAFM to manage the switch from in-band. The only information required for the OSMS interface is the OSMS key.



Fabrics

- 1000080088A0406F
- 1000080088A0A28D
- 1000080088E0AC6B

Product Configuration

NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

API □ Enable Authentication

Method: Local Only

□ Include Current Server

Permitted Software: Server ID

OSMS □ Enable Authentication

OSMS Key:

Retype Key:

Figure 105 Security Center Software tab

Enabling API authentication

If API authentication is enabled, follow these guidelines:

- There must be a minimum of one entry in the Permitted Software box. If not, a warning message is displayed when you click **Apply**.
- The current HAFM appliance must be included. If not, the appliance loses manageability and you are forced to use an alternate management interface to disable API authentication. If you click **Apply** or **Apply To** without including the appliance in the permitted list, a message is displayed, indicating that you must include the appliance in the Permitted Software list before enabling API authentication.
- The current HAFM appliance cannot be deleted. If you remove the current appliance with API authentication turned on, and you click **Apply** or **Apply To**, a message is displayed, indicating that the current server ID cannot be removed when API authentication is enabled.
- Do not delete the last user in the database. If you do, a warning message is displayed, indicating that the last software ID cannot be removed when API authentication is enabled.

For the Authentication method, the following applies:

- Use the **Method** list to select **Local Only**, **Radius Only**, or **Local then Radius**. The default is **Local Only**.

- If you select **Radius Only**, the HAFM appliance checks to see whether a RADIUS server is specified on the **Radius Servers** tab. If not, the **Radius Only** and **Radius then Local** options are not available from the drop-down menu.
- If one RADIUS server is set to **Radius Only**, then the **Radius then Local** option is available.
- The HAFM appliance cannot automatically populate API information to the RADIUS server. A message is displayed, indicating that you have set API Authentication Method to **Radius Only**. If you have not properly defined the software on the RADIUS server, API authentication will fail and the connectivity between software and product will be broken.

The ID and CHAP Secret must be defined for the HAFM appliance so that:

- After you enable API authentication, then the HAFM appliance is not locked.
- If mutual authentication is required between software and switch, a software ID is required. The HAFM appliance is given a default ID during installation. Accept the default or provide another ID name. The software ID must be unique. If the same ID is used, the new ID is rejected and the name must be changed.

Disabling API authentication on the switch

If API authentication is not enabled on a switch, the HAFM appliance can manage the switch if an MPI link with the switch is established. If the HAFM appliance is not licensed with SANtegrity Security Center, launch the Element Manager to add this appliance to the Permitted Software list for the switch.

Adding the current HAFM appliance to the Permitted Software List

The Permitted Software List displays software IDs that are allowed to access the switch through API.

1. To manage the switch, add the current HAFM appliance to the Permitted Software list by selecting the Include Current Server check box.

   If the current appliance does not have a CHAP Secret defined, a message is displayed, indicating that you have not defined a CHAP Secret for this appliance.

   If a CHAP Secret is defined, click **OK** to add the current HAFM appliance to the Permitted Software List.
2. To define a CHAP Secret for the HAFM appliance, click **OK** to display the Server Properties dialog box. If you click **Cancel**, the Software tab is displayed with the check box not selected. The HAFM appliance cannot be added without the CHAP Secret defined.
3. Define the CHAP Secret, and then click **OK** on the Server Properties dialog box to return to the Software tab.
4. Click **Apply** or **Apply To** to populate the CHAP Secret and server ID to the selected switch or switches. When the current server ID is stored in the switch, the Include Current Server check box is disabled but still selected. The check box can be enabled only if the current HAFM appliance is removed from the Permitted Software List.

Removing the current HAFM appliance

To remove the current HAFM appliance, do one of the following:

- If the server ID is defined only on the HAFM appliance and has not been added to the switch, the current appliance can be removed by not selecting the Include current server check box. If the current appliance is selected, Remove is disabled.
- If the server ID and CHAP Secret have been added to the switch, highlight the current appliance and click **Remove**. If the current appliance is removed from the Permitted Software List, the Include current server check box is enabled.

Editing the CHAP Secret for the current HAFM appliance

To edit the CHAP Secret for the current HAFM appliance:

1. Select the appliance and click **Edit**.

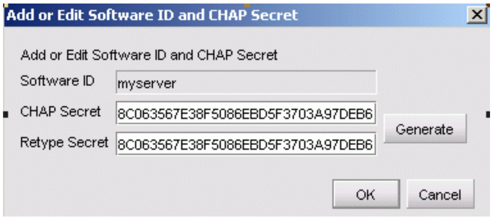
   A message is displayed, indicating that you must use the Server Properties dialog box to edit the current appliance's properties.
2. Click **OK** to display the Server Properties dialog box.
3. Edit the server ID or CHAP Secret.

   If you change the server ID, a message is displayed, indicating that when you change the server ID, you must also update the authenticating switches or the appliance becomes out-of-sync and the switches cannot be managed.
4. Click **OK** to return to the Software tab.

Adding an additional HAFM appliance

1. To add another HAFM appliance to the Permitted Software List, click **Add**.

   The Add or Edit Software ID and CHAP Secret dialog box is displayed (Figure 106).



Add or Edit Software ID and CHAP Secret

Add or Edit Software ID and CHAP Secret

Software ID: myserver

CHAP Secret: 8C063567E38F5086EBD5F3703A97DEB6

Retype Secret: 8C063567E38F5086EBD5F3703A97DEB6

Figure 106 Add or Edit Software ID and CHAP Secret dialog box

2. Enter a unique Software ID.
3. Click **OK**.

   The Software tab is displayed with an asterisk next to the current server ID on the Permitted Software List.

Editing the CHAP Secret for another HAFM appliance

To edit the CHAP Secret for another HAFM appliance in the Permitted Software List:

1. Select the HAFM appliance and click **Change**.

   The Add or Edit Software ID and CHAP Secret dialog box is displayed.

If you modify a CHAP Secret for a non-local server on the Software tab, a message is displayed indicating you are about to modify the CHAP Secret of this HAFM appliance the switch's local database. The message also says to check the Server Properties dialog box for this switch and make sure the secret is updated accordingly. If you fail to do so, this appliance cannot manage the products any more.

2. Edit the CHAP Secret.
3. Click **OK** to return to the Software tab.

Removing another HAFM appliance

Although you can remove software IDs from the Permitted Software List, you cannot remove the last entry in the list while the API authentication is enabled.

Enabling OSMS authentication

OSMS is a PFE key-dependent feature. If the license key is not installed, then OSMS authentication is not available.

Applying changes and confirmation

To apply the change:

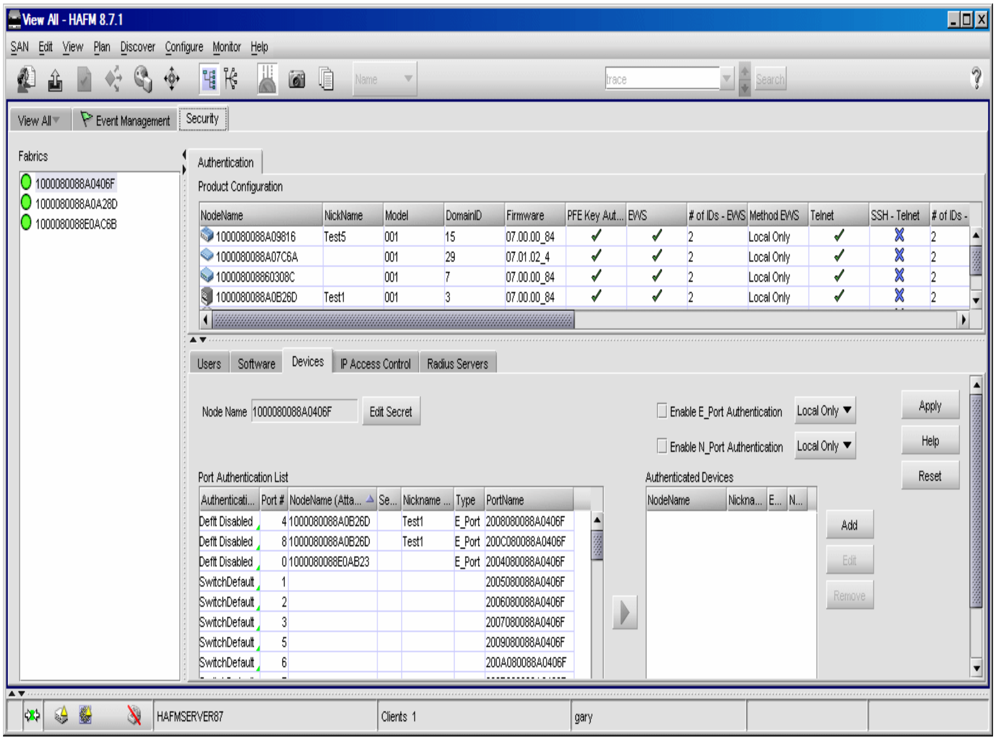
1. From the Software tab, click **OK** on the **Apply** or **Apply To** dialog box.

   The Security Change Confirmation and Status dialog box is displayed. This dialog box is similar to the dialog box that is displayed from the Users tab. The only difference is the Detailed Change table. This table displays the difference between the current settings of the Software tab and the to-be-populated new settings. The behavior of this dialog box is the same as the dialog box for the Users tab.
2. Click **Start**.

If there are no security settings being changed and you click **Apply** or **Apply To**, the To Security Change Confirmation and Status dialog box is displayed with a message indicating no changes were found. Click **Start** and a message is displayed in the Status window indicating the security settings are identical and that there are no changes to apply.

Using the Devices tab

The Devices tab (Figure 107) defines which switches and directors are eligible to mutually authenticate with the highlighted switch on the top table. The features on the Devices tab can be configured only if the switch has the proper PFE key installed. If not, when you click the Devices tab, a message is displayed, indicating that the feature has not been installed.



Product Configuration

NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

Node Name 1000080088A0406F

□ Enable E_Port Authentication Local Only

□ Enable N_Port Authentication Local Only

Port Authentication List

Authenticati...	Port #	NodeName (Atta...	Se...	Nickname ...	Type	PortName
Deflt Disabled	4	1000080088A0B26D		Test1	E_Port	2008080088A0406F
Deflt Disabled	8	1000080088A0B26D		Test1	E_Port	200C080088A0406F
Deflt Disabled	0	1000080088E0AB23			E_Port	2004080088A0406F
SwitchDefault	1					2005080088A0406F
SwitchDefault	2					2006080088A0406F
SwitchDefault	3					2007080088A0406F
SwitchDefault	5					2009080088A0406F
SwitchDefault	6					200A080088A0406F

Authenticated Devices

NodeName	Nickna...	E...	N...

Figure 107 Security Center Devices tab

For two connected switches to authenticate each other locally, each switch must have its own user ID, node WWN, and CHAP Secret, as well as the other switch's user ID and CHAP Secret. The switch can store more IDs and CHAP Secrets if it has multiple connections with other switches only. You can also store IDs and CHAP Secrets of switches that have no physical connections with this switch. This is not recommended because accessing one switch provides access to all switches' CHAP Secrets.

For two connected switches to authenticate each other through the RADIUS server only, all product IDs and CHAP Secrets are stored on the RADIUS server and the product local database is not required to maintain the same data. In this case, the HAFM appliance does not communicate with the RADIUS server effectively. The **Radius Only** authentication method can cause more errors and performance problems.

When you select the **Radius Only** option, the HAFM appliance ensures that only the CHAP Secret for the switch is defined and stored in the local database. If not, a message is displayed, indicating that you must type or generate a secret for the current switch before you enable E_Port authentication.

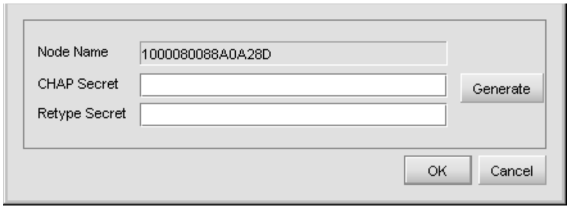
If the CHAP Secret is defined for the current switch, when you click **Apply**, a message is displayed, indicating that you have set E/N_Port Authentication Method to **Radius Only**. If you have not properly defined the secrets for all participating devices on the RADIUS Server, E/N_Port authentication fails and your fabric connectivity is lost.

Understanding the Devices tab display and default settings

When you access the Devices tab:

1. Ensure that the node name is already discovered and displayed in a uneditable text box.
2. Define the CHAP Secret for the selected switch:
   a. Click **Edit Secret**.

      The Add Device dialog box is displayed (Figure 108).



Node Name 1000080088A0A28D

CHAP Secret

Retype Secret

Figure 108 Add Device (Edit Secret) dialog box

   b. Click **Generate** to automatically generate a CHAP Secret and place it in the CHAP Secret and Retype Secret boxes.

      Or

      Type the secret in the CHAP Secret box and retype that Secret in the Retype Secret box.

   c. Click **OK**.
3. If the initial state of a fabric is not configured to enable device authentication, the Enable E_port authentication check box is disabled. To enable, click the Enable E-port Authentication check box.
4. Click the list to the right of the check box and select **Local Only**, **Radius then Local**, or **Radius Only**.

   The default is **Local Only**, which causes the switch to only check its local database to verify if the switch on the other end is allowed to communicate when authentication occurs.
5. If the initial state of a fabric is not configured to enable device authentication, the Enable N_port authentication check box is disabled.

   To enable, click the Enable N-port Authentication check box.
6. Click the list to the right of the check box and select **Local Only**, **Radius then Local**, or **Radius Only**.

   The default is **Local Only**, which causes the switch to check its local database only to verify that the switch on the other end is allowed to communicate when authentication occurs.
7. Check the Port Authentication List. Each table column can be sorted and the column position can adjusted. All the ports are sorted by port number and display in that order.
8. Select a port on the switch to override the authentication settings for that port. Port settings include the following:
   - If a port is configured to be Force Enabled, the port participates in authenticating the other end of the link regardless of the authentication state set at the switch level.
   - If a port is configured to be Force Disabled, that port does not participate in authentication at any time.

- If a port is specified as Switch default, this port abides by all authentication settings configured for this switch. All ports are set to this state at product initialization time.

The HAFM appliance displays all the switches, directors, and end nodes connected to the highlighted switch in the Devices tab. This tracks the security settings on each switch port and the state of connected devices. This list can include:

- Non-SANtegrity II compatible switches
- Non-manageable switches
- Non-HP switches
- JBOD
- HBA
- Other storage devices

When your HAFM appliance is installed with SANtegrity and you discover a secure or unsecure fabric, the E_Port authentication is disabled, and the drop-down menus for port authentication display your HAFM appliance. If a device is SANtegrity capable, your HAFM appliance can discover its current security settings and display them on the table. If not, your HAFM appliance displays only a limited information about that device.

The Authenticated Devices list displays a list of authenticated devices that are in the current switch local database. In this database, there are connected or detached devices. Devices listed in this table must have a CHAP Secret.

Add an attached or detached device from the left Port Authentication List table by selecting a device and clicking the right arrow button, double-clicking the device, or clicking **Add**. Change the CHAP Secret of a device by selecting the device and clicking **Edit**. To remove devices from this list, select a device or multiple devices, and click **Remove**.

NOTE: If the device is involved with the authentication process and the device is removed, the connectivity breaks.

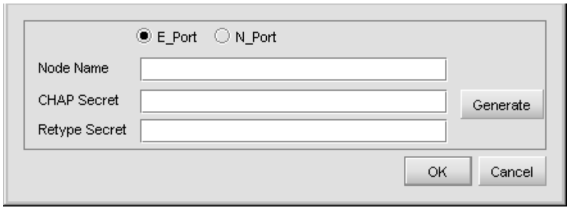
Adding a detached switch

To add a detached switch:

1. Click **Add**.

   The Add Device dialog box is displayed (Figure 109 on page 182).

To add a device that is not discovered by the HAFM appliance, a device that is not physically connected, or a device that is discovered but not directly attached to the current switch.



● E_Port ○ N_Port

Figure 109 Add Device dialog box

2. Type the node name.
    - If node name is already in the Authenticated Devices list or is invalid, the new entry is rejected.
    - If the node name is in the Port Authentication list as a connected device, the device can be transferred from the Port Authentication list to the Authenticated Devices list.
    - If the node name is not in the Authenticated Devices list, but is discovered in the fabric and has CHAP Secret, a message is displayed.
    - If the node name is not in the Authenticated Devices list, but is discovered in the fabric, and the CHAP Secret is not known because the device is not manageable or is an HBA, a message is displayed.
3. Click **OK**.

    The added devices are displayed in the Authenticated Devices list in the order in which the devices were added.
4. To edit the CHAP Secret for the device, select the device and click **Edit**.

    When editing a device's CHAP Secret, all other devices that participate in authentication with this device must have the local database refreshed, or the connectivity is lost.

Populating a CHAP Secret to a current switch

1. Select a CHAP Secret for the current switch.
2. Click **Apply** to populate the CHAP Secret in the current switch.

Changing a CHAP Secret for a switch

1. To modify a predefined CHAP Secret for the current switch, click **Apply**.

    A confirmation message is displayed that asks if you want to modify the CHAP Secret.
2. Click **Yes** to modify the CHAP Secret of the current switch and populate the CHAP Secret to all other connected and authenticating devices.

Adding a connected device with CHAP Secret to a switch

1. Select a device in the Port Authentication table.
2. Click the right arrow.

    The device is moved to the Authenticated Devices list.

Adding a connected device without a CHAP Secret to a switch

1. Select a device in the Port Authenticated Devices table.
2. Click the right arrow.

   The Add User dialog box is displayed.

Changing a CHAP Secret for a connected device

1. Select a connected device from the Authenticated Devices list and click **Edit**.

   The Change Secret dialog box is displayed
2. Click **OK**.
3. The CHAP Secret for the device is changed inside the local database, and in the current switch's Authenticated Devices list.

Removing a connected device from a switch

1. Select a connected device from the Authenticated Devices list.
2. Click **Remove**.

Changing a CHAP Secret for a detached device

1. Select a device and click **Edit**.

   The Add User dialog box is displayed.
2. Click **OK** and the CHAP Secret for the device is updated in the current local database for the switch. This device is not actively authenticating with the current switch, so the CHAP Secret needs to be changed for this device locally and for other affected devices.

Removing a detached device from a switch

1. Select a detached device and click **Remove**.

   The detached device is not actively authenticating with the current switch, so it is removed.

Enabling or disabling E_Port and N_Port authentication

Select or clear the check box for E_Port or N_Port authentication.

The port authentication state overrides the E_Port and N_Port authentication at the switch level.

Changing the Enable Authentication method

Select an option from the Enable Authentication Method list for E_Port or N_Port.

- If the **Radius Only** option is selected, and E_Port or N_Port authentication is enabled, the application checks to see if the RADIUS server settings on the Radius tab have been set.
- If not, the **Radius Only** and **Radius** then **Local** options do not display on the list.

Changing the port authentication state for an authenticated device

1. Select a device and choose a different port authentication state.

   If the device is already in the authenticated device list, changing the port authentication state can occur.

Changing the port authentication state for a nonauthenticated device with or without a CHAP Secret

1. Select a device, and select Force Enabled or Switch Setting from the corresponding authentication state while the E_Port authentication is checked.

   If the device has not been transferred to the Authenticated Devices list, Needed is displayed in the Secret column whether the device has a CHAP Secret or not.
2. Continue configuring multiple port authentication states.
3. Click **Apply**.

   A message is displayed indicating the devices have not been put into the Authenticated Devices list and as a result the connectivity between the devices and the switch is broken.
4. Click **Yes**. The authentication is enabled between the current switch and the connected devices with switch ports set to Enabled.

   Or

   Click **No** and return to the Devices tab where you can add the devices to the Authenticated Devices list.

Changing the port authentication state for a nonmember device (manageable) without a CHAP Secret

If the port authentication state is changed to Forced Enabled or Switch Setting from the corresponding authentication state while the E_port authentication is checked, the Secret column changes its display value from `No` to `Needed`.

1. Double-click the corresponding Secret column or select the device and click the right arrow button to display the Add User dialog box.
2. Select the CHAP Secret, and then click **OK**.

   The corresponding Secret column displays `Set`. The device is added to the Authenticated Devices list. The secret is populated to both the device's local database and the current switch's Authenticatable list.

Changing the port authentication state for a nonmember device that is not managed

1. Select the E_port authentication check box for a device that is not manageable.
2. Change the port authentication state to Force Enabled or Switch Settings.

   The Secret column changes from `No` to `Needed`.
3. Double-click the corresponding Secret column to display the Add User dialog box.
4. Type the CHAP Secret.
5. Click **OK**.

   The Secret column for that device displays `Set`. The device is added to the Authenticated Devices list. The secret is populated to the current switch's Authenticated Devices list.
6. Access the device that is not managed and populate the same Secret into the local database.

Applying changes and confirmation

1. Click **Apply** from the Devices tab.

   The Security Change Confirmation and Status dialog box is displayed.

This dialog box is similar in behavior to the Security Change Confirmation and Status that is displayed from the Users tab. The only difference is in the Detailed Changes table. On the Devices tab there is no **Apply To** available, so there is always one product in the Product List. This table displays the difference between the current settings of the Devices tab and to-be-populated new settings.

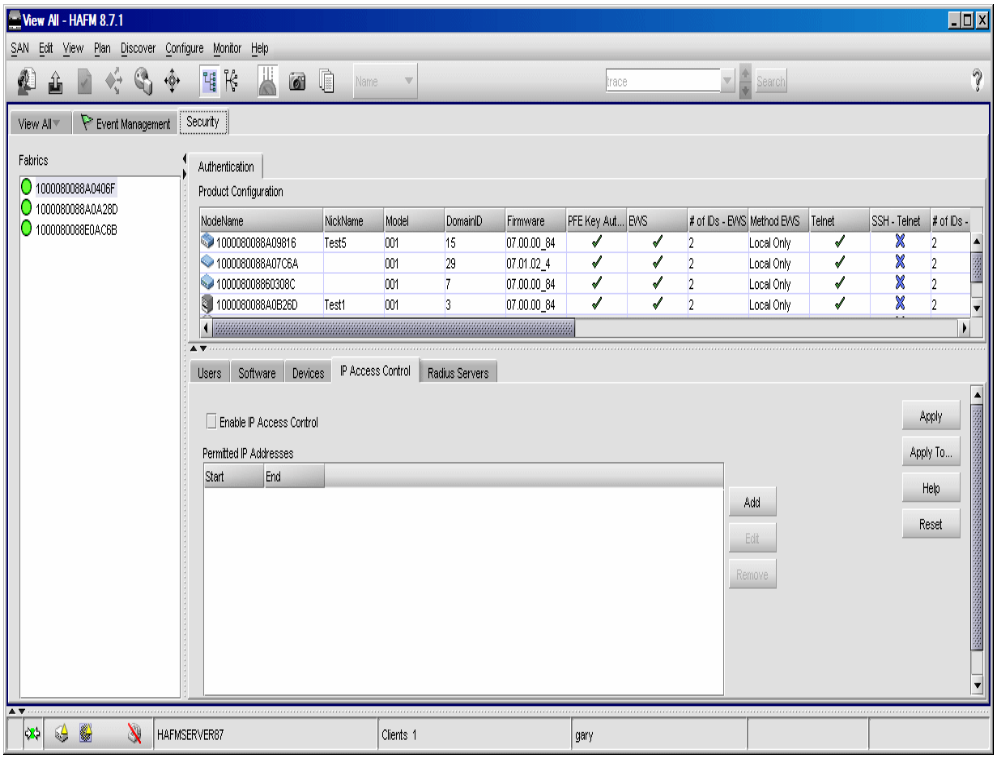
2. Click **Apply** even if there are no security settings being changed.

   If there are no security settings being changed, the Security Change Confirmation and Status dialog box is displayed with the Detailed Changes table showing that `No Changes were Found` on the first row.

3. Click **Start** and the status window displays a message indicating the security settings are identical and there are no changes to apply.

IP Access Control list tab

The IP Access Control tab (Figure 110) contains IP addresses of the devices that are allowed to manage the switch. IP addresses that are not on this list cannot manage the switch from the IP management port.



Product Configuration

NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

☐ Enable IP Access Control

Permitted IP Addresses

Start	End

Figure 110 Security Center IP Access Control tab

If the Enable IP Access Control List check box is selected, the restricted access to the follow IP addresses is enforced. If not checked, management interfaces can access the switch from any IP address. The check box is enabled only if at least one IP address is in the list.

Adding a new IP address

1. Click **Add**.

   The Add/Edit IP Address or Range dialog box is displayed.
2. Enter an IP Address or an IP Address Range.

   The IP range is defined by a starting IP address and ending IP address.
3. Click **Apply**.

Editing one IP address or one range of IP addresses

1. Click **Change**.

   The Add/Edit IP Address or Range dialog box is displayed.
2. Change the IP address or IP Address Range.
3. Click **Apply**.

NOTE: If multiple IP addresses or ranges are selected, **Edit** is disabled.

Removing multiple IP addresses at one time

After adding, changing or removing IP addresses, to set the IP Access Control List, perform one of the following:

- Click **Apply** and the changes are reflected for that switch in the Product Configuration table.
- Click **Apply To** and a dialog box with a list of switches is displayed.
- Click Reset and all the changes are dropped and the settings revert to the values that were set before the changes.

The IP address of the HAFM appliance is not a default included in this list. When accessing the IP ACL tab, the Enable IP ACL check box is not selected. You cannot remove the server IP address from the Permitted IP Addresses list while the Enable IP ACL check box is selected. To remove the server IP from the list, disable the IP ACL.

Applying changes and confirmation

1. Click **Apply** from the IP ACL tab.

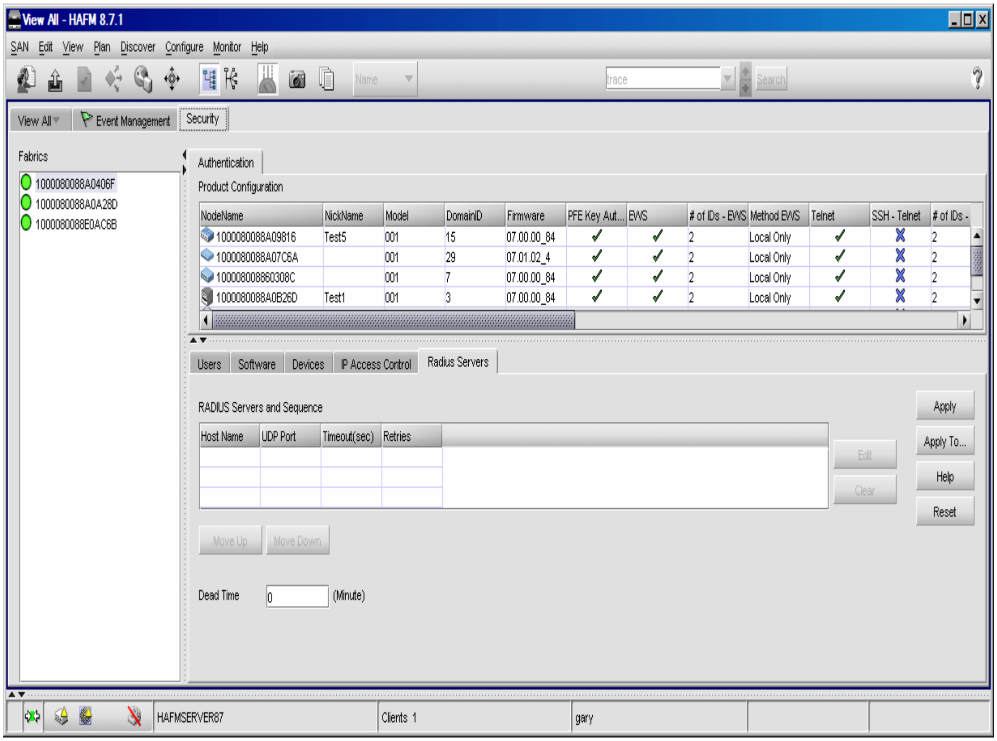
   The Security Change Confirmation and Status dialog box is displayed.

   This dialog box is similar in behavior to the Security Change Confirmation and Status that is displayed from the Users tab. The only difference is in the Detailed Changes table. This table displays the difference between the current settings of IP ACL tab and to-be-populated new settings.
2. Click **Apply** or **Apply To** even if there are no security settings being changed.

   If there are no security settings being changed, the Security Change Confirmation and Status dialog box is displayed with the Detailed Changes table showing that `No Changes were Found` on the first row.
3. Click **Start** and the status window displays a message indicating the security settings are identical and there are no changes to apply.

RADIUS Servers tab

The Radius Servers tab (Figure 111) allows you to specify the RADIUS server that will be used for authentication.



NodeName	NickName	Model	DomainID	Firmware	PFE Key Aut...	EWS	# of IDs - EWS	Method EWS	Telnet	SSH - Telnet	# of IDs -
1000080088A09816	Test5	001	15	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A07C6A		001	29	07.01.02_4	✓	✓	2	Local Only	✓	✗	2
100008008860308C		001	7	07.00.00_84	✓	✓	2	Local Only	✓	✗	2
1000080088A0B26D	Test1	001	3	07.00.00_84	✓	✓	2	Local Only	✓	✗	2

Host Name	UDP Port	Timeout(sec)	Retries

Dead Time 0 (Minute)

Figure 111 Security Center Radius Servers tab

You can specify up to three RADIUS servers per switch. The device that must be authenticated by the RADIUS server always is display ed at the top of the table. If the first device does not respond after a certain amount of time due to connection or configuration problems, the next device is authenticated, and so on.

The RADIUS servers and Sequence table includes information about the following:

- The Host Name can be an IP Address.
- The UDP Port displays the number that the device uses to contact the RADIUS server. The port number is `1812` by default.
- The Time out(sec) displays the amount of time to wait for a response from the RADIUS server before retransmitting the packet. It can be `1` to `1000`; the default is `2` seconds.
- The Retries column specifies the number of times a packet is sent to a RADIUS server if a response is not received before the timeout. After the retransmit limit is reached, the Gateway switches to the next server. The value can be `1` to `100`; the default is `3` attempts.
- The Dead Time setting located below the RADIUS servers and Sequence table apply to all available RADIUS servers. If a RADIUS server does not respond to an authentication request, it can be marked as `dead` for a specified time interval. This can speed up authentication by

eliminating timeouts and retransmissions. If no alternate RADIUS servers are available, which means that only one server is configured or that all servers are marked as dead, the dead time is ignored. The dead time can be `0` to `1440` minutes; the default is `0`.

- Click **Edit** to display the Add/Edit Radius Server dialog box. Use this dialog box to define all the settings that display in the RADUIS Servers and Sequence table.
- Select one or more RADIUS servers and click **Clear** to clear the settings.
- Adjust the sequence of RADIUS servers by using the Move Up and Move Down buttons.
- Click **Reset** to reverse the settings to the initial settings that displayed when the tab was first accessed.

Applying changes and confirmation

1. Click **Apply** from the Radius Servers tab.
2. The Security Change Confirmation and Status dialog box is displayed.

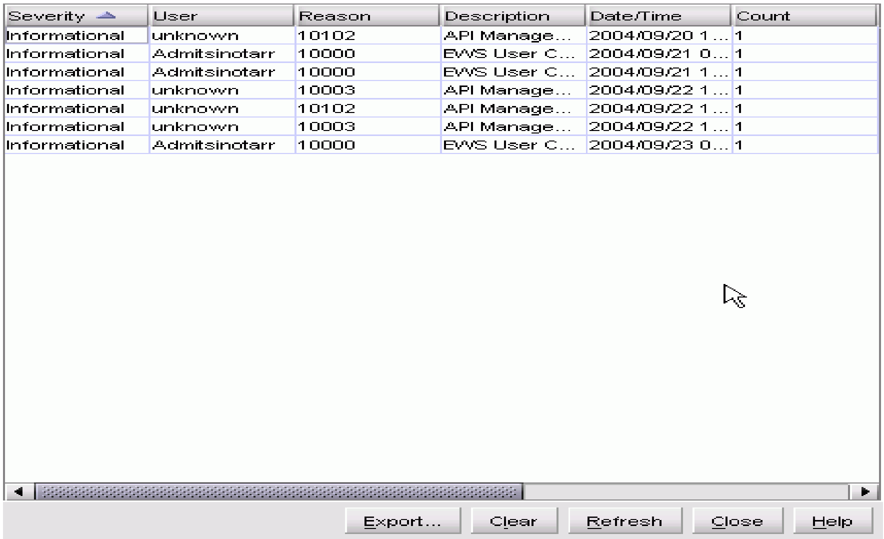
   This dialog box is similar in behavior to the Security Change Confirmation and Status that is displayed from the Users tab. The only difference is in the Detailed Changes table. This table displays the difference between the current settings of the Radius Servers tab and the to-be-populated new settings.
3. Click **Apply** or **Apply To** even if there are no security settings being changed.

   If there are no security settings being changed, the Security Change Confirmation and Status Servers dialog box is displayed with the Detailed Changes table showing that `No Changes were Found` on the first row.
4. Click **Start** and the status window displays a message indicating the security settings are identical and there are no changes to apply.

Viewing the Security Log

You must log in as the Security Administrator or System Administrator to view the Security Log. The Security Log can be viewed from the following:

- On the HAFM main window, click the Security tab. The Security Log is displayed (Figure 112 on page 190) as a table at the bottom of the window.
- On the HAFM main window, select **Monitor > Log > Security Log**. The Security Log dialog box is displayed (Figure 112 on page 190).
- On the Element Manager main window, select **Logs > Security Log**. The Security Log dialog box is displayed (Figure 112 on page 190).



Severity	User	Reason	Description	Date/Time	Count
Informational	unknown	10102	API Manage...	2004/09/20 1 ...	1
Informational	Admitsinotarr	10000	EWS User C...	2004/09/21 0...	1
Informational	Admitsinotarr	10000	EWS User C...	2004/09/21 1 ...	1
Informational	unknown	10003	API Manage...	2004/09/22 1 ...	1
Informational	unknown	10102	API Manage...	2004/09/22 1 ...	1
Informational	unknown	10003	API Manage...	2004/09/22 1 ...	1
Informational	Admitsinotarr	10000	EWS User C...	2004/09/23 0...	1

Figure 112 Security Log

Columns in the Security Log are:

- **Severity**—The severity level of the event: informational, warning, or fatal.
- **User**—The user associated with the event.
- **Reason**—The reason code for the failure.
- **Description**—Provides details of the event and the IP address of the product.
- **Date/Time**—The date and time that the event occurred. The format is `yyyy/mm/dd hh:mm:ss:tt`. The last two characters (hundredth of seconds) are for advanced logs with a higher frequency rate.
- **Count**—The number of times that the same event occurs.
- **Category**—The category of the event.
- **IP**—The IP address of the switch.
- **Role**—The role of the user.
- **Interface**—The interface.

Table 24 lists the Security Log reason codes:

Differences between the SANtegrity Security Center and the SANtegrity Authentication

The SANtegrity Security Center for your HAFM appliance that manages the fabric is similar to the SANtegrity Authentication for the Element Manager that manages a single product. The following differences between the two occur because one manages the fabric while the other manages a single product.

- The SANtegrity Security Center is accessed by a license key and the SANtegrity Authentication accessed on the Element Manager is not accessed by a license key.

- The SANtegrity Security Center is accessed from a tab that is parallel to the View tab in the main window. The SANtegrity Authentication is accessed from the Configure menu.
- The SANtegrity Security Center displays a Product Configuration table that lists all discoverable products and their security settings. The SANtegrity Authentication display does not have this table.
- The SANtegrity Security Center Users tab displays an **Apply To** button. The SANtegrity Authentication Users tab does not have this button.
- The SANtegrity Security Center Software tab displays an **Apply To** button. The SANtegrity Authentication Software tab display does not have this button.
- The SANtegrity Security Center Devices tab populates CHAP Secrets to the local switch and the connected devices. The SANtegrity Authentication Devices tab populates CHAP Secrets to the local switch.
- The SANtegrity Security Center IP ACL tab displays an **Apply To** button. The SANtegrity Authentication IP ACL tab display does not have this button.
- The SANtegrity security Center Radius tab displays an **Apply To** button. The SANtegrity Authentication Radius tab display does not have this button.
- The SANtegrity Security Center Security Change Confirmation and Status tab displays multiple switches in addition to the local switches. The SANtegrity Authentication Security Change Confirmation and Status tab displays only the local switch.

A Configuring HAFM through a firewall

Networks can use a virtual private network (VPN) or firewall to prohibit communication between servers and clients. This appendix provides optional procedures for configuring HAFM client and server applications to function across remote networks through a firewall.

This appendix describes the following topics:

- Polling mode, page 195
- TCP port numbers, page 197

Polling mode

Generally, the server calls the client when it has new data. If the client uses firewall technology, the server can be unable to reach the client. In this case, the HAFM application automatically detects the network configuration and runs the client in polling mode.

When the client is running in polling mode, the server queues up the data and the client periodically (approximately every 5 or 10 seconds) checks in and retrieves the data. The original two-way communication is transformed into one-way client-controlled communication, allowing passage through firewalls.

Decreasing login time

When a client attempts to log in to a server, the server typically calls back to verify communication. In a firewall situation, this call fails and the server then treats the client as a polling client. It can take up to 45 seconds for this call-back to fail. You can configure a polling parameter in client and server batch files to identify the client as a polling client. The causes the server to skip the call-back step and shortens the login time.

Forcing a client to polling mode

To force a client to be a polling client, add the `-Dsmp.callback.passive` parameter to the following files in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`):

- Client portion of the `HAFM_sc.bat` file
- `HAFM_c.bat` file

The `HAFM_sc.bat` file starts both the client and server and is installed on a computers with the HAFM appliance software. The `HAFM_c.bat` file starts the client only and is installed with the client software.

The following example shows the edited files with the additional parameter in **bold**. This parameter only affects the specified client.

NOTE: This example illustrates the `HAFM_c.bat` file. The portion of this file starting with `rem HAFM Client` is also included in the `HAFM_sc.bat` file. Both files must be modified if they are installed on your computer.

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
rem HAFM Client
start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15 -Xmaxf.35 -classpath
%CLASSPATH%-Dsun.java2d.noddraw=true -Dsmp.fabricPersistenceEnabled=true
-Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/ -Dsmp.callback.passive
-Dsmp.flavor=%APP_FLAVOR% Client

rem HAFM Client Debug Mode
rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsun.java2d.noddraw=true -Dsmp.fabricPersistenceEnabled=true
-Dsmp.deployment.prefix=Client/ -Dsmp.debug -Dsmp.callback.passive
?Dsmp.flavor=%APP_FLAVOR% Client
popd
endlocal
```

Forcing all clients to polling mode

To force all clients communicating with a server to be treated as polling clients (regardless of the parameters the clients launch with), add the `-Dsmp.callback.passive` parameter to the HAFM server section of the `HAFM_sc.bat` file located in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`).

The following example shows the edited files with the added parameter in **bold**:

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
...............
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xm512m
-Xminf.15 -Xmaxf.35 -classpath %CLASSPATH%
-Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer -Dsmp.callback.passive
-Dsmp.flavor=%APP_FLAVOR% Server

rem HAFM Server Debug Mode
rem start %JAVA_HOME%\bin\HAFMServerD.exe -server
-Xmx512m -Xminf.15 -Xmaxf.35 -classpath
%CLASSPATH% -Dsun.java2d.noddraw=true -Dsmp.Mp.max=512
-Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=legacy
```

```
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug
-Dsmp.webServer -Dsmp.callback.passive
-Dsmp.flavor=%APP_FLAVOR% Server
...............
:end
popd
endlocal
```

TCP port numbers

This section provides information about configuring TCP port numbers for remote management interface (RMI) servers and registries to allow HAFM client and server application to function across firewalls.

HAFM function with RMI at TCP port level

The HAFM appliance communicates with clients through the RMI server (Figure 113). This is a full-duplex function. However, the HAFM client must know the TCP/IP port number of the RMI server on the HAFM appliance before they can communicate. The RMI registry communicates this TCP port number to the HAFM client. The HAFM appliance obtains the TCP port number of the RMI Server on the client during initial communications.

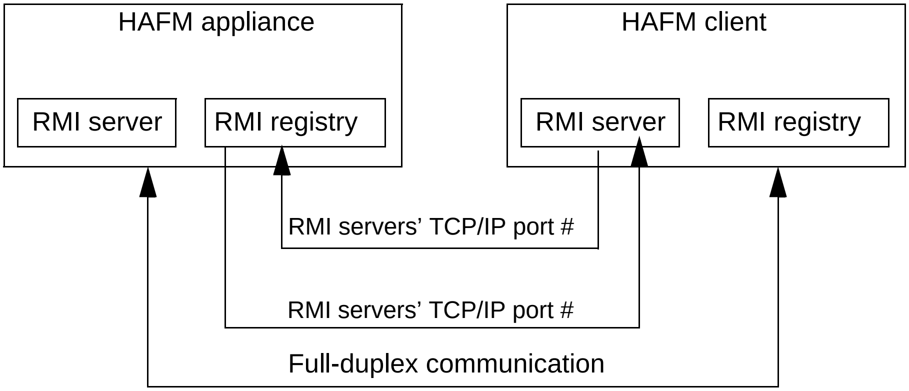

HAFM appliance
RMI server
RMI registry
HAFM client
RMI server
RMI registry
RMI servers' TCP/IP port #
RMI servers' TCP/IP port #
Full-duplex communication

Figure 113 HAFM appliance and client communications

The TCP port numbers of the RMI server are randomly and automatically selected on both the HAFM appliance and client as a full-duplex function. Firewalls are configured to block all unknown incoming connections with no mapping of outgoing connections based on a socket part of TCP and IP.

To work around this problem, administrators can configure the port numbers into appropriate batch files, and then configure the firewall to unblock the configured port numbers. The procedure that you follow depends on how the firewall is set up:

- If the firewall prevents the client from connecting to arbitrary ports on the server, then perform the following procedures:
  - "Forcing the RMI registry to use a specific port" on page 198

- ”Forcing the server and client to export a port number” on page 199

NOTE: You must configure both the server and client export port numbers.

- If the firewall prevents the server from connecting to arbitrary ports on the client, then configure the export port of the client in ”Forcing the server and client to export a port number” on page 199.

Forcing the RMI registry to use a specific port

To force the RMI registry to use a specific TCP port for an RMI server, configure the `Dsmp.registry.port=XXXX` parameter in the following files in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`):

- The client and server portion of the `HAFM_sc.bat` file
- `HAFM_c.bat` file (if installed)

The `HAFM_sc.bat` file starts both the client and server and is installed on a computers with the HAFM appliance software. The `HAFM_c.bat` file starts the client only and is installed with the client software.

HAFM_sc.bat

Place the parameter `-Dsmp.registry.port=`*`XXXX`*, where *`XXXX`* is any TCP port number not being used by another application after the `%CLASSPATH%` parameter.

The following example shows the edited file with the added parameter in **bold**:

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
...............
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer -Dsmp.registry.port=XXXX
-Dsmp.flavor=%APP_FLAVOR% Server
rem HAFM Server Debug Mode
rem start %JAVA_HOME%\bin\HAFMServerD.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH%
-Dsmp.Mp.max=512 -Dsmp.autodiscovery=false -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug -Dsmp.webServer
-Dsmp.registry.port=XXXX
-Dsmp.flavor=%APP_FLAVOR% Server
:client
rem HAFM Client
start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15 -Xmaxf.35 -classpath
%CLASSPATH% -Dsun.java2d.noddraw=true -Dsmp.fabricPersistenceEnabled=true
```

```
-Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/ -Dsmp.registry.port=XXXX
?Dsmp.flavor=%APP_FLAVOR% Client
rem HAFM Client Debug Mode
rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug -Dsmp.registry.port=XXXX
?Dsmp.flavor=%APP_FLAVOR% Client
:end

popd
endlocal
```

HAFM_c.bat

The `HAFM_c.bat` file starts the client only. Edit file to include the parameter `-Dsmp.registry.port=XXXX`, where `XXXX` is any TCP port number not being used by another application. You must place this parameter after the `%CLASSPATH%` parameter.

The following example shows the edited file with the added parameters in **bold**:

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
...............
rem HAFM Client
start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15 -Xmaxf.35 -Xincgc
-classpath %CLASSPATH% -Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/
-Dsmp.flavor=HAFM Client


rem HAFM Client Debug Mode
rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15 -Xmaxf.35
-Xincgc -classpath %CLASSPATH% -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/-Dsmp.debug -Dsmp.registry.port=XXXX
-Dsmp.flavor=HAFM Client


popd
endlocal
```

Forcing the server and client to export a port number

To force the server and client to export a specific TCP port number for an RMI server:

1. Configure the following parameters in the `HAFM_sc.bat` file:

   -`Dsmp.server.export.port=`*XXXX*

   -`Dsmp.client.export.port=`*YYYY*

2. Configure the `-Dsmp.client.export.port=`*YYYY* parameter in the `HAFM_c.bat` file.

These files are located in the `HAFM 8.x\bin` directory (typically in `c:\Program Files\HAFM 8.x\bin`).

The HAFM_sc.bat file starts both the client and server and is installed on a computers with the HAFM appliance software. The HAFM_c.bat file starts the client only and is installed with the client software.

NOTE: If the firewall prevents the server from connecting to arbitrary ports on the client, then just force the export port of the client (-Dsmp.client.export.port=YYYY).

HAFM_sc.bat

Place the parameter -Dsmp.server.export.port=*XXXX* in the server area of the file, and the parameter -Dsmp.client.export.port=*YYYY*, in the client area of the file, where *XXXX* and *YYYY* are any TCP port numbers not used by another application. Although the server port number *XXXX* could match the client port number *YYYY*, this is not necessary. Add the parameters after the %CLASSPATH% parameter.

The following example shows the edited file with the added parameters in **bold**:

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
...............
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.server.export.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server
rem HAFM Server Debug Mode
rem start %JAVA_HOME%\bin\HAFMServerD.exe -server -Xmx512m -Xminf.15
-Xmaxf.35 -classpath %CLASSPATH% -Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.debug -Dsmp.webServer
-Dsmp.server.export.port=XXXX -Dsmp.flavor=%APP_FLAVOR% Server
:client
rem HAFM Client
start %JAVA_HOME%\bin\HAFMClient.exe -Xmx256m -Xminf.15 -Xmaxf.35 -classpath
%CLASSPATH% -Dsun.java2d.noddraw=true -Dsmp.fabricPersistenceEnabled=true
-Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/
-Dsmp.client.export.port=YYYY ?Dsmp.flavor=%APP_FLAVOR% Client
rem HAFM Client Debug Mode
rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsun.java2d.noddraw=true
-Dsmp.fabricPersistenceEnabled=true -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug -Dsmp.client.export.port=YYYY
?Dsmp.flavor=%APP_FLAVOR% Client
:end
popd
endlocal
```

HAFM_c.bat

HAFM_c.bat starts the client only. HAFM_c.bat starts the client only and is installed with the client software. Edit the file to include the parameter -Dsmp.client.export.port=YYYY. Add this parameter after the %CLASSPATH% parameter.

The following example shows the edited file with the added parameters in **bold**:

```
setlocal
pushd %~dp0\..
call bin\set_cp.bat
...............
rem HAFM Client
start %JAVA_HOME%\bin\HAFMMClient.exe -Xmx256m -Xminf.15 -Xmaxf.35 -Xincgc
-classpath %CLASSPATH% -Dsmp.Mp.max=256 -Dsmp.deployment.prefix=Client/
-Dsmp.flavor=HAFM Client


rem HAFM Client Debug Mode
rem start %JAVA_HOME%\bin\HAFMClientD.exe -Xmx256m -Xminf.15 -Xmaxf.35
-Xincgc -classpath %CLASSPATH% -Dsmp.Mp.max=256
-Dsmp.deployment.prefix=Client/ -Dsmp.debug -Dsmp.client.export.port=YYYY
-Dsmp.flavor=HAFM Client


popd
endlocal
```

B Troubleshooting

This appendix provides troubleshooting information for the following:

- Problems with discovery, page 203
- Problems with products, page 205
- Problems with addresses, page 205
- Miscellaneous problems, page 211
- Problems with zoning, page 212

Problems with discovery

Table 25 describes possible problems with discovery and suggested resolutions.

Table 25 Discovery problems and resolutions

Problem	Resolution
Discovery is turned off.	Select **Discover > On**.
Devices are not being discovered.	Ensure that your SNMP communication parameters are set correctly in order to discover switches.
Discovered devices are not being displayed.	Specify each device in the Out-of-Band dialog box, either by the individual IP address or by subnet. **1.** Select **Discover > Setup**. **2.** Add, change, and remove IP addresses, as necessary. See "Configuring IP addresses and community strings" on page 76. **3.** Select IP addresses from the Available Addresses list and add them to the Selected Subnets or Selected Individual Addresses lists by clicking ▷ . If you add addresses to the Selected Subnets list, select a method (Broadcast or Sweep). **4.** Click **OK**.
	Ensure that you've selected to view the fabric that includes the discovered devices.
	Ensure that only one copy of the application is being used to monitor and manage the same devices in a subnet.
Cannot see HBA in discovery setup bos	HAFM requires specific HBA driver levels. Verify driver levels.

Table 25 Discovery problems and resolutions (continued)

Problem	Resolution
Broadcast request is blocked by routers.	**Resolution 1:** If you know the IP addresses, and they are not in the Available Addresses list: 1. Select **Discover > Setup**. 2. Click **Add**. 3. Enter data in the dialog box. 4. Click **OK**. 5. Repeat steps step 1 through step 4 until all addresses are available. 6. Select the IP addresses you would like to discover in the Available Addresses list. 7. Click ▷ to move your choices to the Selected Individual Addresses list. 8. Click **OK**. **Resolution 2:** If you know the IP addresses and the addresses are listed in the Available Addresses list: 1. Select **Discover > Setup**. 2. Select the IP addresses you would like to discover in the Available Addresses list. 3. Click ▷ to move your choices to the Selected Individual Addresses list. 4. Click **OK**. **Resolution 3:** This method significantly increases your discovery time. If you don't know the specific IP addresses: 1. Select **Discover > Setup**. 2. Click the Method column for the selected subnet in the Selected Subnets list and select **Sweep**. 3. Click **OK**.
Discovery time is excessive.	**Resolution 1:** 1. Select **Discover > Setup**. 2. Click the Method column in the Selected Subnets pane and select **Broadcast**. 3. Click **OK**. **Resolution 2:** Decrease the SNMP timeout to decrease the discovery time.
Cannot open an Element Manager for an HP device.	Ensure that only one copy of the application is being used to monitor and manage the device.
The `symapi.jar` file is not in the class path.	Verify that the `symapi.jar` file has been copied to HAFM's `lib` directory.

Problems with products

Table 26 describes possible product problems and suggested resolutions.

Table 26 Product problems and resolutions

Problem	Resolution
HBAs not connected to SAN.	Check your physical cables and connectors.
Switches not connected to Ethernet.	Check your physical cables and connectors.
Switches not connected to SAN.	Check your physical cables and connectors.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	Disable the Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Fabric Binding.

Problems with addresses

Table 27 describes possible problems with addresses and suggested resolutions.

Table 27 Address problems and resolutions

Problem	Resolution
No subnets or addresses selected	1. Select **Discover > Setup**. 2. Click the subnet or individual address you would like to discover in the Available Addresses list. 3. Click ▶ to move your choice to the Selected Subnets list, or to the Selected Individual Addresses list. 4. Click **OK**.
Wrong IP addresses selected	1. Select **Discover > Setup**. 2. Verify that the IP addresses in the Selected Subnets and Selected Individual Addresses lists are the correct current addresses for the SAN. 3. Click **OK**.
Wrong community strings selected	1. Select **Discover > Setup**. 2. Select an IP address. 3. Click **Change**. 4. Select the desired community strings. 5. Click **OK**.

Table 27 Address problems and resolutions (continued)

Problem	Resolution
The application cannot currently manage LUNs on this device.	Verify the following conditions have been met: • Check the discovery setup. • Verify that discovery is not still in progress. • Verify that the management application is installed in the appropriate path. If ESSCLI or NaviCLI is not available, events will be generated indicating that HAFM is not available. • Verify that the device you've selected is a supported device configuration • Verify that the device is online. • Verify that the management server is running. For ESS systems, the web server should be running on the ESS and be accessible from the machine running the server. To test this, from the machine running the server, open an web browser. In the address bar, type `http://ipaddress_of_ESS_machine`. When the StorWatch application starts, open a command prompt and type esscli -u userid -p passwd -s ipaddress list server, using the user ID and password you entered in the Discover Setup dialog box for the ESS and the IP address of the ESS. Verify that the command returns meaningful data. On Symmetrix systems: • Verify that the SYMAPI server is running and can be contacted from the system running the HAFM server. • Verify that the SYMAPI is licensed for LUN Management.
Communication with the storage management application failed.	Verify the following conditions have been met: • Verify that the device is online. • Verify that the management server is running. For ESS, the web server should be running on the ESS and be accessible from the machine running the server. To test this, from the machine running the server, open an web browser. In the address bar, type http://ipaddress_of_ESS_machine. When the StorWatch application starts, open a command prompt and type `esscli -u userid -p passwd -s ipaddress list server`, using the user ID and password you entered in the Discover Setup dialog box for the ESS and the IP address of the ESS. Verify that the command returns meaningful data.

Table 27 Address problems and resolutions (continued)

Problem	Resolution
LUN Management actions failed.	Verify the following conditions have been met: • Verify that the device is online. • Verify that the management server is running. For ESS, the web server should be running on the ESS and be accessible from the machine running the server. To test this, from the machine running the server, open an web browser. In the address bar, type http://ipaddress_of_ESS_machine. When the StorWatch application starts, open a command prompt and type `esscli -u userid -p passwd -s ipaddress list server`, using the user ID and password you entered in the Discover Setup dialog box for the ESS and the IP address of the ESS. Verify that the command returns meaningful data. • Verify that the client is communicating with the server. • Verify that a green server connection indicator is displayed on the status bar. • Verify that the LUN data configuration was not changed while the dialog box was open. On Symmetrix systems: • Verify that the SYMAPI server is running and can be contacted from the system running the HAFM server. • Verify that the required SYMCLI licenses are installed. To perform LUN querying, the EMC Solutions Enabler Base Component License must be installed. To perform LUN masking and Port Binding, the EMC Solutions Enabler Configuration Manager License must be installed. • Verify that the system running the SYMAPI server is running and is connected to a Symmetrix port through in-band.
LUN query failed on Symmetrix systems.	To perform LUN querying, the EMC Solutions Enabler Base Component License must be installed.
LUN masking failed on Symmetrix systems.	To perform LUN masking, the EMC Solutions Enabler Configuration Manager License must be installed.
Port Binding failed on Symmetrix systems.	To perform Port Binding, the EMC Solutions Enabler Configuration Manager License must be installed.

Table 27 Address problems and resolutions (continued)

Problem	Resolution
The LUN Management box is displayed as empty.	Verify that the application has finished collecting LUN data before opening the LUN Management dialog box. On Symmetrix systems: • Verify that the WideSky API is not installed on the system running the HAFM appliance. • Verify that the SYMAPI server is running and can be contacted from the system running the HAFM appliance. • Verify that the system running the SYMAPI server is running and is connected to a Symmetrix port through in-band.

Table 27 Address problems and resolutions (continued)

Problem	Resolution
LUN Management is not available on HP-UX systems.	The LUN management feature is not currently supported on HP-UX systems. It is only available on Windows, Solaris, and AIX systems.
Encountering errors when performing LUN management on HDS systems.	1. Make sure the HiCommand Device Manager (server) is online. 2. Ensure that communication between HiCommand Device Manager and the storage array is intact. When the HiCommand Device Manager cannot communicate to the device, the following error will display: An error was encountered during this operation. Some of the operation can have been applied to the storage subsystem. A refresh of the storage subsystem is recommended. Please contact your System Administrator if you are a local user. 3. To make sure HiCommand server is able to communicate to the storage device, launch HiCommand GUI and refresh the array. See the following documents on HiCommand Device Manager for HiCommand installation, GUI usage, and error codes: • *Hitachi HiCommand Device Manager Server Installation and Configuration Guide* • *Hitachi HiCommand Device Manager Web Client User's Guide* • *Hitachi HiCommand Device Manager Error Codes*

Table 27 Address problems and resolutions (continued)

Problem	Resolution
Encountering errors when performing LUN management on HDS 9980 V systems.	The host domains on this HDS 9980 V must be reconfigured using the native software before can manage the LUNs. The same LUN or host port is included in two host domains on the same port. • The HDS 9980 V, in conjunction with HiCommand Server 2.4, supports a new feature, which is not yet supported in 4.2. • This new feature allows you to create multiple host domains on the same storage port, which include the same LUNs or host ports. • 4.2 only supports the previous HDS V series configuration rules. • For each storage port, any given LUN can only be a member of a single host storage domain. For each storage port, any given host port can only be a member of a single host storage domain. • To manage your 9980 V LUNs with 4.2, any preexisting host domains that do not conform to these two rules, must be reconfigured or removed using the HiCommand Server 2.4 or greater. • When the rules are met, 4.2 will discover all the host domains and allow you to configure them. • If rules 1 & 2 are not met, 4.2 can discover all the LUNs, and their host assignments. • The data displayed in the LUNs and Hosts tables will be correct. • The Troubleshoot tab can be used to diagnose the connectivity between LUNs and host ports. • The host domain data will be incomplete. Therefore, the dialog will be in a browse only mode. • No actions can be taken on a HDS 9980 V that has been configured in this way until its host storage domains are reconfigured to meet rules 1 and 2 above.

Miscellaneous problems

Table 28 describes possible miscellaneous problems and suggested resolutions.

Table 28 Miscellaneous problems and resolutions

Problem	Cause/resolution
Code Execution Error: Array Index Out-Of-Bounds.	Retry the command or action. If the problem persists, contact HP customer support.
Code Execution Error: Internal Exception	Retry the command or action. If the problem persists, contact HP customer support.
Code Execution Error: Missing Property File.	Retry the command or action. If the problem persists, contact HP customer support.
Code Execution Error: Invalid Product Type.	Retry the command or action. If the problem persists, contact HP customer support.
The server doesn't start.	Examine the server log (`*Install_Home*\Server\Universe_Home\TestUniverse\_Working\EventStorageProvider\event.log)` for diagnostic information.
Server to client communication is inhibited.	The network can be utilizing virtual private network (VPN) or firewall technology. See Appendix A for more information.
Data and settings are not imported during installation.	Open an MS-DOS window and enter the following script at the command line: Install_Service <*startstatus* > <*runnow*>. The `startstatus` parameter is *`manual`* or *`auto`* and `runnow` parameter is *`true`* or *`false.`*
Windows service does not display correctly in the Computer Management (Windows 2000) or Service Control Manager (Windows NT) window.	You installed or uninstalled the Win32 service while the Computer Management or Service Control Manager window was open. Close the window and reopen it to see the changes.
An error is displayed stating that the application failed to setup the *`serverinit.txt`* or *`.license`* file.	Delete the *`Install_Home`*`\Server\serverinit.txt` file or the *`Install_Home`*`\Server\Config\Other\.license` file and rerun the installer.
The product does not install on a Windows system.	Verify that the system has 100 MB available on the C drive. The program requires 100 MB for installation, but only 50 MB to run.
Mapping a loop to a hub causes the loop group and the outermost portion of the topology's background group color or layout format to revert to the default.	Make the background and/or layout changes after mapping the loop to the hub.

Table 28 Miscellaneous problems and resolutions (continued)

Problem	Cause/resolution
Using Fabric Manager or Device Manager to manage Cisco MDS9xx switches.	Install JRE 1.4 or greater, which includes Java Web Start
When the client application is started on an HP-UX machine, the exception `java.lang.OutOfMemoryError: unable to create new native thread` is displayed in thread *`main`*.	The following two HP-UX 11.0 kernel parameters are set too low for most Java applications. Edit the parameter limits as described below. max_thread_proc: Increase the maximum number of threads allowed in each process higher than the expected maximum number of simultaneously active threads (for example, 1024). The maximum value is the value of nkthread. nkthread: Set the limit for the total number of kernel threads able to run simultaneously in the system to a value greater than `nproc`. The default is approximately twice that of `nproc`. The maximum is 30000.
The system reboots or is unable to gather SNMP information.	Multiple SNMP calls are being sent to a device that can't handle the constant requests for information. Verify that the devices you are discovering are not being discovered by another appliance. Discovering devices using multiple appliances can result in errors.
A report failed to be generated due to memory constraints.	Generate a fewer number of reports at one time.
Receiving error `Compatibility between <`*`TARGET VERSION`*`> and <`*`CURRENT VERSION`*`> is unknown. Do you want to continue?`	Firmware files are included in the upgrade process, but release rules are not. Since release rules are required when sending another firmware version to a switch, this error results. To fix this problem, add the latest firmware file to the firmware library. This also adds the new release rules and resolves the problem.
An error occurs when trying to delete a nickname.	Once assigned, a nickname cannot be deleted.
The system reboots or is unable to gather SNMP information.	Multiple SNMP calls are being sent to a device that can't handle the constant requests for information. To resolve this issue, verify that the devices you are discovering are not being discovered by another server. Discovering devices using multiple servers can result in errors.

Problems with zoning

The following section states some possible issues and recommended solutions for zoning errors.

Table 29 Zoning problems and resolutions

Problem	Cause/resolution
Receiving zoning errors.	Verify that you did not configure zoning on a non-principal switch.
The application is not performing zoning discovery very often.	Zoning discovery is performed once at startup, and then once every two hours during routine discovery. If the Zoning dialog box is open, zoning discovery is performed during every polling cycle. It continues to discover at the increased speed for 30 minutes before it returns to the default value.
When activating a large zone set on a two-switch fabric on UNIX platforms, an error message is displayed stating `Failed to perform the requested zoning action: Failed to zone due to exception COM.hp.hafmecc.HafmUnavailableException`.	Although the error message states that the requested zoning action failed, the zone set correctly activated. Wait for the next zoning polling to occur.
Zoning activation message is displayed for a long time, but zone set is not activated.	Telnet zoning can take a long time. To improve speed, open the Discover Setup dialog box and add the HAFM IP address for HP switches to the Selected Individual Addresses list.
When opening the Zoning dialog box from a particular switch or fabric, the message `Cannot zone the selected device or fabric` is displayed.	The application can have been unable to log in to the fabric due to another active session. Verify that there is not another active session. The application cannot support zoning on any of the discovered products.

C Informational and error messages

This appendix lists informational and error messages that are displayed by the HAFM application and the associated Element Managers.

The first section of the appendix lists HAFM application messages. The second section lists Element Manager messages. The text of each message is followed by a description and recommended course of action.

HAFM application messages

This section lists HAFM application informational and error messages in alphabetical order.

Table 30 HAFM Messages

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone using the Modify Zone dialog box.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set using the Modify Zone dialog box.
All alias, zone, and zone set names must be unique.	When creating a new alias, zone, or zone set, the name must be unique.	At the New Zone dialog box, choose a unique name for the new alias, zone, or zone set.
All zone members are logged.	Attempt was made to display all zone members not logged in using the **Zone Set** tab, but all members are currently logged in.	Informational message.
An HAFM application session is already active from this workstation.	Only one instance of the HAFM application is allowed to be open per remote workstation.	Close all but one of the HAFM application sessions.
Are you sure you want to delete this network address?	The currently-selected network address will be deleted.	Click **Yes** to delete or **No** to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click **Yes** to delete the nickname or **No** to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click **Yes** to delete the product or **No** to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click **Yes** to delete the user or **No** to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click **Yes** to delete the zone or **No** to cancel the operation.

Table 30 HAFM Messages (continued)

Message	Description	Action
Are you sure you want to delete this zone set?	The selected zone set will be deleted from the zone library.	Click **Yes** to delete the zone set or **No** to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click **Yes** to overwrite or **No** to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click **Yes** to delete the members or **No** to cancel the operation.
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding WWN for the device you want to add to the zone.
Cannot connect to management server.	The HAFM application at a remote workstation could not connect to the HAFM appliance.	Verify the HAFM appliance IP address is valid.
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM appliance-to-product link is up. If the link is up: • The HAFM appliance can be busy. • Another Element Manager instance can be open. • You cannot have permission to delete the product.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You attempted to disable Fabric Binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in the HAFM application before disabling Fabric Binding.
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM appliance.	Make sure devices named in Show Routes dialog box are attached to products managed by this HAFM appliance.

Table 30 HAFM Messages (continued)

Message	Description	Action
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Edge Switch 2/16s, Edge Switch 2/32s, Director 2/64s, or Director 2/140s.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route on one switch fabric.	You cannot show routes between end devices in a fabric when configuring Show Routes (Configure menu).	Error is displayed when attempting to show routes on a fabric with only one switch. Configure Show Routes on a multiswitch fabric.
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this box.	Delete spaces from the box entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then modify the name through the Modify Zone Set dialog box.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then modify the name through the Modify Zone Set dialog box.

Table 30 HAFM Messages (continued)

Message	Description	Action
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM appliance-to-product link is up. If the link is up: • The HAFM appliance can be busy. • Another Element Manager instance can be open. • You cannot have permission to modify the product.
Cannot perform operation. Fabric is unknown.	This message is displayed if no switches in the fabric are connected to the HAFM appliance.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	This message is displayed when attached nodes are unavailable and you attempt to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name has not been configured.	Enter a valid community name in the Configure SNMP dialog box.
Cannot show zoning library. No fabric exists.	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to the HAFM application for a fabric to exist.	Identify an existing switch or director to the HAFM application using the New Product dialog box.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
Connection to management server lost.	The connection to the remote HAFM appliance has been lost.	Log in to the HAFM appliance again through the HAFM Log In dialog box.

Table 30 HAFM Messages (continued)

Message	Description	Action
Connection to management server lost. Click OK to exit application.	The HAFM application at a remote workstation lost the network connection to the HAFM appliance.	Restart the HAFM application to connect to the HAFM appliance.
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk can be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Change the Interop Mode from Open Fabric to Homogeneous using the Configure Fabric Parameters dialog box. You can also redefine zone members by the device WWN.
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other devices in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
Download complete. Click OK and start the HAFM.	Download of HAFM and the Element Manager is complete.	Start the HAFM application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Choose another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.

Table 30 HAFM Messages (continued)

Message	Description	Action
Duplicate World Wide Name in nickname configuration.	A WWN can be associated with only one nickname.	Modify (to make it unique) or delete the selected WWN.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Element Manager instance is currently open.	A product cannot be deleted while an instance of the Element Manager is open for that product.	Close the Element Manager, then delete the product.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced.	Click **OK** to continue or **Cancel** to end the operation.
Error connecting to switch.	While viewing routes, the HAFM appliance was unable to connect to the switch. The switch failed or the switch-to-HAFM appliance Ethernet link failed.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The HAFM application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.

Table 30 HAFM Messages (continued)

Message	Description	Action
Error removing zone or zone member.	The HAFM application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the HAFM application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding fabric log is deleted.	Click **Yes** to unpersist the fabric or **No** to cancel the operation.
Fabric member could not be found.	A fabric member does not exist when the application prepared to find a route, find a route node, or gather route information on that fabric member.	Ensure the product is incorporated into the fabric and retry the operation. If the problem persists, contact the next level of support.
Fabric not persisted.	You attempted to refresh or clear the log, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Click **OK** to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.
Field cannot be blank.	The data box requires an entry and cannot be left blank.	Enter appropriate information in the data box.
File transfer aborted.	You aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
HAFM error <error number 1 through 8 >.	The HAFM application encountered an internal error (1 through 8 inclusive) and cannot continue operation.	Contact the next level of support to report the problem.
Management server could not log you on. Verify your username and password.	An incorrect username or password (both case sensitive) was used while attempting to log in to the HAFM application.	Verify the username and password with the customer's network administrator and retry the operation.

Table 30 HAFM Messages (continued)

Message	Description	Action
Management server is shutting down. Connection will be terminated.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the data box.	Remove invalid characters from the entry.
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Choose a valid name and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0–31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Choose a valid product and retry the operation.

Table 30 HAFM Messages (continued)

Message	Description	Action
Invalid request.	Three conditions result in this message: You tried to add or modify a product from Product View and the network address is already in use. (Network addresses must be unique.) You tried to create a new user with a username that already exists. (A username must be unique.) You tried to delete the default Administrator user. (The default Administrator user cannot be deleted.)	Choose the action that is appropriate to the activity that caused the error: Network address: Specify a unique network address for the product. username: Specify a unique username for the new user ID. Do not delete the default Administrator user.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.
Invalid World Wide Name.	The specified WWN format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Enter a WWN using the correct format.
Invalid World Wide Name or nickname.	The WWN or nickname that you have specified is invalid. The valid format for the WWN is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid WWN or nickname.

Table 30 HAFM Messages (continued)

Message	Description	Action
Invalid World Wide Name. Valid WWN format is: xx:xx:xx:xx:xx:xx:xx:xx.	The specified WWN format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Retry the operation using a valid WWN or nickname.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
Limit exceeded.	You cannot add a new product or user to HAFM application if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
No address selected.	You cannot complete the operation because an address has not been selected.	Choose an address and retry the operation.
No attached nodes selected.	An operation was attempted without an attached node selected.	Choose an attached node and try the operation again.
No management server specified.	An HAFM appliance is not defined to the HAFM application.	At the HAFM Log In dialog box, type an appliance name in the Server Name box and click **Login**.
No nickname selected.	No nickname was selected when the command was attempted.	Choose a nickname and try again.
No Element Managers installed.	No director or switch Element Manager is installed on this workstation.	Install the appropriate Element Manager to this workstation.
No routing information available.	No information is available for the route selected.	Choose a different route and try the operation again.
No user selected.	A user was not selected when the command was attempted.	Choose a user and try again.

Table 30 HAFM Messages (continued)

Message	Description	Action
No zone member selected.	A zoning operation was attempted without a zone member selected.	Choose a zone member and try the operation again.
No zone selected.	A zoning operation was attempted without a zone selected.	Choose a zone and try the operation again.
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Choose a zone and try the operation again.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only—no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Choose a zone set and try the operation again.
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Choose a zone set and try the operation again.
Only attached nodes can be displayed in this mode.	You cannot display unused ports when adding ports by WWN.	Change the add criteria to Add by Port.
Password and confirmation don't match.	Entries in the password box and confirmation password box do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the Remote Access dialog box are allowed to connect to the HAFM appliance.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.

Table 30 HAFM Messages (continued)

Message	Description	Action
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM appliance was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the Remote Access dialog box.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance can be busy. Try the operation again later.
Route data corrupted.	The information for this route is corrupt.	Try the operation again. If the problem persists, contact the next level of support.
Route request timeout.	The Show Route request timed out.	Try the operation again. If the problem persists, contact the next level of support.
Routing is not supported by the switch.	This switch or director does not support the Show Routes feature.	Choose a different switch or director to show the route.
SANtegrity Feature not installed. Please contact your sales representative.	You selected **Fabric Binding** or **Enterprise Fabric Mode** from the Fabrics menu. These selections are not enabled because the optional SANtegrity binding feature is not installed.	Install the SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode.
Select alias to add to zone.	An alias was not selected before clicking **Add**.	Choose an alias before clicking **Add**.
Selection is not a World Wide Name.	The selection made is not a WWN.	Choose a valid WWN before performing this operation.
Server shutting down.	The HAFM application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.

Table 30 HAFM Messages (continued)

Message	Description	Action
Switch is not managed by HAFM.	The selected switch or director is not managed by the HAFM application.	Choose a different switch or director.
The Administrator user cannot be deleted.	The administrator user is permanent and cannot be deleted from the Configure Users dialog box.	Informational message only—no action is required.
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but a switch already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the Add Detached Switch dialog box.
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager and cannot perform the requested operation.	Wait until the process completes, then perform the operation again.
The link to the managed product is not available.	The Ethernet connection between the HAFM appliance and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of aliases has already been configured.	The maximum number of aliases allowed was reached.	Delete an existing alias before adding a new alias.
The maximum number of management server network addresses has already been configured.	The number of HAFM appliance IP addressees that can be defined to the HAFM application has already been configured.	Delete an existing IP address before adding a new address.
The maximum number of members has already been configured.	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete an existing zone member before adding a new zone member.

Table 30 HAFM Messages (continued)

Message	Description	Action
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the HAFM application was reached.	Delete an existing nickname before adding a new nickname.
The maximum number of open products has already been reached.	The maximum number of open switches allowed was reached.	Close an Element Manager session (existing open product) before opening a new session.
The maximum number of products has already been configured.	The number of managed HP switches (48) that can be defined to the HAFM application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of managed HP switches of this type (48) that can be defined to the HAFM application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum number of eight IP addresses for remote workstations can be configured at the Session Options dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of users has already been configured.	The number of users (32) that can be defined to the HAFM application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.

Table 30 HAFM Messages (continued)

Message	Description	Action
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this management server is not compatible with the version on the remote management server.	A second HAFM appliance (client) connecting to the HAFM appliance must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM appliance.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected fabric log is no longer available because the fabric has been unpersisted.	To start a new log for the fabric, persist the fabric through the Persist Fabric dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this management server.	The product selected is not managed by this HAFM appliance.	Choose a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product.
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	You attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.

Table 30 HAFM Messages (continued)

Message	Description	Action
This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	You attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the Fabric Membership List with the same WWN.	Enter a unique WWN for the switch in the Add Detached Switch dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the management server software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click OK to install a compatible version.	The HAFM application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance.	Download a compatible version of the HAFM application to the remote workstation (client) using the web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required using the Configure Users dialog box.
You must define an SMTP server address.	An SMTP server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the Configure E-Mail dialog box.
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the Configure E-Mail dialog box.
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the Remote Access dialog box.

Table 30 HAFM Messages (continued)

Message	Description	Action
You must download the HAFM client via the web install.	An attempt was made to download the HAFM application to a remote workstation (client) using an improper procedure.	Download a compatible version of the HAFM application to the remote workstation (client) using the web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through WWNs.	Informational message only–no action is required.
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for HAFM.	Define zones using the New Zone dialog box.
Zoning by port number is ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through WWNs.	Informational message only–no action is required.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if HAFM is in Open Fabric Mode.	Either define zones by WWN of device or change to Homogeneous Fabric mode in the Configure Operation Mode dialog box of the Element Manager.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Element Manager messages

This section lists Element Manager informational and error messages in alphabetical order.

Table 31 Element Manager messages

Message	Description	Action
A Preferred Path already exists between this Source Port and this Destination Domain ID. Please reconfigure the desired path.	For any source port, only one path can be defined to each destination domain ID.	On the Add/Change Preferred Path dialog box, change the preferred path.
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click **Yes** to confirm activating the new address configuration or **No** to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All FPM ports will be held inactive while the director is configured to 2 Gb/sec speed. Do you want to continue?	Occurs when FPM cards are installed in the director and director speed is being set to 2 Gb/sec in the Configure Switch Parameters dialog box.	Replace FPM cards with UPM cards (UPM cards operate at 1 and 2 Gb/sec) or set the director speed to 1 Gb/sec.
All port names must be unique.	A duplicate Fibre Channel port name was configured. All port names must be unique.	Reconfigure the Fibre Channel port with a unique name.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
An Element Manager instance is already open.	Only one instance of the Element Manager can be open at one time.	Close the open Element Manager so the desired instance of the Element Manager can be opened.
Another Element Manager is currently performing a firmware install.	Only one instance of the Element Manager can install a firmware version to the director at a time.	Wait for the firmware installation process to complete and try the operation again.

Table 31 Element Manager messages (continued)

Message	Description	Action
Are you sure you want to delete firmware version?	This message requests confirmation to delete a firmware version. Firmware library can store up to 8 firmware versions.	Click **Yes** to delete the firmware version or **No** to abort the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click **Yes** to confirm the deletion of the address configuration or **No** to cancel the operation.
Are you sure you want to send firmware version?	This message requests confirmation to send a firmware version from the HAFM appliance's firmware library to the director. Firmware library can store up to 8 firmware versions.	Click **Yes** to send the firmware version or **No** to abort the operation.
Cannot change Port Type while Management Style is FICON without SANtegrity feature. Please contact your sales representative.	Firmware is below the required level and you attempted to change a port type in the Configure Ports dialog box while FICON management style, but the optional SANtegrity Binding feature is not installed.	Informational message. If the firmware is below the required level, install SANtegrity Binding before changing port types in the Configure Ports dialog box while in FICON management style.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	You attempted to disable Switch Binding through the Switch Binding Change State dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the Enterprise Fabric Mode dialog box in the HAFM application or set the switch offline before you can disable Switch Binding.
Cannot disable Insistent Domain ID while Fabric Binding is active.	You attempted to disable the Insistent Domain ID parameter through the Configure Switch Parameters dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the Fabric Binding dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot enable beaconing while the system light is on.	Occurs when choosing Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on an operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select **Clear System Error Light** from **Product** menu to clear error light, then enable beaconing.
Cannot enable Open Trunking while Enterprise Fabric Mode is active and the switch is offline.	Enterprise Fabric mode is active and the switch or director is online and you attempted to enable Open Trunking. This message is displayed if the optional Open Trunking feature is installed.	Perform either of the following steps: Disable Enterprise Fabric Mode option by selecting the appropriate fabric in the Fabric Tree portion of the HAFM Manager window (Fabrics tab) and then selecting **Enterprise Fabric Mode** from the **Fabrics** menu. When the Enterprise Fabric Mode dialog box is displayed, click **Start** and follow prompts to disable the feature. Set the switch or director offline through the Set Online State dialog box. Display this dialog box by selecting **Set Online State** from the Element Manager **Maintenance** menu.
Cannot have E-Ports if Management Style is FICON unless SANtegrity feature is installed. Please contact your sales representative.	Firmware is below the required level and you attempted to change management style from Open Systems to FICON management style with E_Ports configured, but SANtegrity Binding is not installed.	Informational message. If firmware is below the required level and you install SANtegrity Binding before changing to FICON management style, then E_Ports will remain as E_Ports when you change to FICON management style. If SANtegrity Binding is not installed, setting a director to FICON management style will change all E_Ports to G_Ports.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this box.	Delete spaces from the box entry.
Cannot install firmware to a director with a failed CTP card.	A firmware version cannot be installed on a director with a failed control processor (CTP) card.	Replace the failed CTP card and retry the firmware installation.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch.
Cannot modify director/switch speed. Ports speeds cannot be configured at a higher data rate than the director/switch speed.	Port speeds cannot be configured at a higher data rate than the director speed. This message is displayed when you set director sped to 1 GB/sec through the Configure Switch Parameters dialog box and at least one of the ports is running at 2 Gb/sec.	Either return the director speed to 2 Gb/sec or configure all port data speeds to 1 Gb/sec through the Configure Ports dialog box.
Cannot perform this operation while the switch is offline.	This operation cannot take place while the director or switch is offline.	Configure the director or switch offline through the Set Offline State dialog box and then retry the operation.
Cannot retrieve current SNMP configuration.	The director SNMP configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve diagnostics results.	Director diagnostic results cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve information for port.	Port information cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port configuration.	The port configuration cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch date and time.	The director or switch date and time cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve switch state.	The director or switch state cannot be retrieved by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot run diagnostics on a port that is failed.	Port diagnostics (loopback tests) cannot be performed on a port that has failed any previous diagnostic (power-on diagnostic, online diagnostic, or loopback test). The amber LED associated with the port illuminates to indicate the failed state.	Reset the port and perform diagnostics again.
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.
Cannot run diagnostics on a port that is not installed.	Port diagnostics cannot be performed on a port card that is not installed.	Run diagnostics only on a port that is installed.
Cannot run diagnostics on a port card that is not installed.	Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor (SFF) optical transceiver installed.	Install a transceiver in the port and perform diagnostics again.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot run diagnostics while a device is logged-in to the port.	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.	Ensure the device is logged out and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	A device is logged in to the port where a diagnostic test is attempted.	Log out the device and run the diagnostic test again.
Cannot save IPL configuration while active=saved is enabled.	You cannot save the IPL file while the active=saved property is set.	The FICON Management Server property, active=save, must be disabled for HAFM to save the IPL file.
Cannot save port configuration.	The port configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot save SNMP configuration.	The SNMP configuration cannot be saved at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set all ports to 1 Gb/sec due to speed restriction on some ports.	Displays if you try to set ports to operate at 1 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.
Cannot set all ports to 2 Gb/sec due to speed restriction on some ports.	Displays if you try to set ports to operate at 2 Gb/sec data speed through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one configuration.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the Configure Ports dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set Fibre Channel parameters.	Fibre Channel parameters for the director cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch date and time.	The switch date and time cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set switch state.	The director or switch state cannot be set at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set write authorization without defining a community name.	A community name was not defined in the Configure SNMP dialog box for the write authorization selected.	Provide a name in the Name box where write authorization is checked.
Cannot start data collection.	The data collection procedure cannot be started by the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start firmware install while CTP synchronization is in progress.	The director's CTP cards are synchronizing and firmware cannot be installed until synchronization is complete.	Install the firmware after CTP card synchronization completes.

Table 31 Element Manager messages (continued)

Message	Description	Action
Cannot start port diagnostics.	Port diagnostics cannot be started at the Element Manager because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot swap an uninstalled port.	A port swap cannot be performed when the port card is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or click **Cancel** to cancel the operation.
Connection to management server lost. Click OK to exit application.	The HAFM application at a remote workstation lost the network connection to the HAFM appliance.	Start the HAFM application to connect to the HAFM appliance.
Continuing may overwrite host programming. Continue?	Configurations sent from the host can be overwritten by HAFM.	Continuing will activate the current configuration, which may have been configured by a FICON host.
Could not export log to file.	A log file I/O error occurred and the file could not be saved to the specified destination. The disk can be full or write protected.	Ensure file name and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory. Or, the selected file is not a firmware file.	Ensure file name and directory are correct. Or, obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be deleted from the HAFM appliance because the link can be down, or the HAFM appliance or Element Manager is busy.	Retry the operation later. If the condition persists, contact the next level of support.
Could not stop port diagnostics.	Port diagnostics could not be stopped by the Element Manager because the Ethernet link is down or busy, or because the director is busy.	Retry the operation later. If the condition persists, contact the next level of support.

Table 31 Element Manager messages (continued)

Message	Description	Action
Could not write firmware to flash.	A firmware version could not be written from the HAFM appliance to FLASH memory	Retry the operation again. If the condition persists, contact the next level of support.
Control Unit Port (CUP) name and port name are identical (FICON ONLY).	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	The date is entered incorrectly at the Configure Date and Time dialog box. Individual box entries can be correct, but the overall date is invalid (for example, a day entry of 31 for a 30-day month).	Verify each entry is valid and consistent.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running.	Terminate the device application and perform diagnostics again.
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	You attempted to remove a device WWN from the Switch Membership List (SANtegrity Binding feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the Switch Binding Change State dialog box before removing devices from the Switch Membership List.
Director clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.

Table 31 Element Manager messages (continued)

Message	Description	Action
Director must be offline to configure.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and you attempted to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through HAFM and you attempted to disable Insistent Domain ID in the Configure Switch Parameters dialog box.	Click **Yes** if you want to continue and disable Fabric Binding.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the **Configure Switch Parameters** dialog box.	Click **Yes** if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	You attempted to disable Switch Binding through the Switch Binding State Change dialog box, but Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Switch Binding.
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the director.	Click **Yes** to IPL the director or **Cancel** to cancel the operation.
Domain IDs must be in the range of 1 to 31.	Domain IDs entered in the Configure Preferred Paths dialog box must fall in a specific range.	In the Configure Preferred Paths dialog box, change the number in the Destination Domain ID box to a number between 1 and 31, inclusive.
Duplicate Community names require identical write authorizations.	Duplicate community names are entered at the Configure SNMP dialog box, and have different write authorizations.	Delete the duplicate community name or make the write authorizations consistent.

Table 31 Element Manager messages (continued)

Message	Description	Action
Element Manager error <number>.	The Element Manager encountered an internal error and cannot continue.	Contact the next level of support to report the problem.
Element Manager instance is currently open.	A Element Manager window is currently open.	Informational message only.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue?	You attempted to disable these parameters in the Configure Switch Parameters dialog box while the switch was online, but Enterprise Fabric Mode (SANtegrity Binding feature) is enabled.	Click **Yes** if you want to continue, and disable Enterprise Fabric Mode.
Error retrieving port information.	An error occurred at the Element Manager while retrieving port information because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error retrieving port statistics.	An error occurred at the Element Manager while retrieving port statistics because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error stopping port diagnostics.	An error occurred at the Element Manager while attempting to stop port diagnostics from running because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the Element Manager. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.

Table 31 Element Manager messages (continued)

Message	Description	Action
Feature not supported. The ‘product name’ must be running version 05.00.00 or higher.	The firmware version on the hardware product (switch or director) is lower than 05.00.00. This message is displayed if the optional Open Trunking feature is installed.	Install firmware version 5.00.00 or higher on the hardware product.
Field cannot be blank.	The data box requires an entry and cannot be left blank.	Enter appropriate information in the Data box.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the box was exceeded.	Enter the information using the prescribed number of characters.
File transfer aborted.	You aborted the file transfer process.	Information message only.
File transfer is in progress.	A firmware file is being transferred from the HAFM appliance hard drive, or a data collection file is being transferred to a CD.	Informational message only—no action is required.
Firmware download timed out.	The director or switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file I/O error.	A firmware download operation aborted because a file I/O error occurred.	Retry the operation. If the problem persists, contact the next level of support.
Firmware file not found.	The firmware version is not installed (or was deleted) from the firmware library at the HAFM appliance.	Add the firmware version to the library and retry the operation.

Table 31 Element Manager messages (continued)

Message	Description	Action
Incompatible configuration between management style and management server.	If the Firmware is below the required level, only FICON management style is allowed if the FICON Management Server feature is enabled. You attempted to enable Open Systems management style.	Disable FICON Management Server, enable the Open Systems Management Server, or enable the Open Systems management style.
Incorrect product type.	When configuring a new product through the New Product dialog box, an incorrect product was specified.	Choose the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is nondisruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM appliance will be lost momentarily, but Fibre Channel traffic will not be affected.	Click **Yes** to install the feature key or **No** to not install.
Internal file transfer error received from director.	The director or switch detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the Data box.	Remove invalid characters from the entry.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens, and underscores.
Invalid feature key.	The feature key was not recognized.	Reenter the feature key. Ensure that you type each character in the correct case (upper or lower), include the dashes, and do not add any spaces at the end.
Invalid firmware file.	The file selected for firmware download is not a firmware version file.	Choose the correct firmware version file and retry the operation.

Table 31 Element Manager messages (continued)

Message	Description	Action
Invalid management server address.	The IP address specified for the HAFM appliance is unknown to the domain name server (invalid).	Verify and enter a valid HAFM appliance IP address.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port address.	Invalid port address has been entered.	Verify port address through the Configure Addresses–"Active" dialog box (FICON management style only) and reenter.
Invalid port number.	The port number must be within a range of ports for the specific director or switch model.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	An error occurred at the switch during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid response received from director.	An error occurred at the director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this director serial number.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number from 1 through 655535.
Invalid value for BB_Credit.	At the Configure Fabric Parameters dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from 1 through 60 inclusive.	Verify and enter a valid number between 1 through 60.

Table 31 Element Manager messages (continued)

Message	Description	Action
Invalid value for Low BB Credit threshold (1-99) %.	Low BB Credit Threshold box in Configure Open Trunking dialog box must have entries in the range from 1 and 99. This message is displayed if the optional Open Trunking feature is installed.	Enter a value from 1 to 99 into the Low BB Credit Threshold box of the Configure Open Trunking dialog box.
Invalid value for day (1-31).	At the Configure Date and Time dialog box, the DD value (day) must be an integer from 1 through 31 inclusive.	Verify and enter a valid date.
Invalid value for E_D_TOV.	At the Configure Fabric Parameters dialog box, the error detect time-out value (E_D_TOV) must be an integer from 2 through 600 inclusive.	Verify and enter a valid number.
Invalid value for hour (0-23).	At the Configure Date and Time dialog box, the HH value (hour) must be an integer from 0 through 23 inclusive.	Verify and enter a valid time.
Invalid value for minute (0-59).	At the Configure Date and Time dialog box, the MM value (minute) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for month (1-12).	At the Configure Date and Time dialog box, the MM value (month) must be an integer from 1 through 12 inclusive.	Verify and enter a valid date.
Invalid value for R_A_TOV.	At the Configure Fabric Parameters dialog box, the resource allocation time-out value (R_A_TOV) must be an integer from 10 through 1200 inclusive.	Verify and enter a valid number.

Table 31 Element Manager messages (continued)

Message	Description	Action
Invalid value for second (0-59).	At the Configure Date and Time dialog box, the SS value (second) must be an integer from 0 through 59 inclusive.	Verify and enter a valid time.
Invalid value for threshold (1-99)%.	Value entered for each port in the Configure Open Trunking dialog box must be in the range from 1 to 99. This message is displayed if the optional Open Trunking feature is installed.	Enter a number from 1 to 99 into the Threshold % column of the Configure Open Trunking dialog box.
Invalid value for year.	At the Configure Date and Time dialog box, the YYYY value (year) must be a four-digit value.	Verify and enter a four-digit value for the year.
Invalid World Wide Name or nickname.	The WWN or nickname that you have specified is invalid. The valid format for the WWN is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid WWN or nickname.
Link dropped.	The HAFM appliance-to-director Ethernet link was dropped.	Retry the operation. Link reconnects are attempted every 30 seconds. If the condition persists, contact the next level of support.
Log is currently in use.	Access to the log is denied because the log was opened by another instance of the Element Manager.	Retry the operation later. If the condition persists, contact the next level of support.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.

Table 31 Element Manager messages (continued)

Message	Description	Action
Maximum number of versions already installed.	The number of firmware versions that can be defined to the HAFM application's firmware library (eight) was reached.	Delete an existing firmware version before adding a new version.
No file was selected.	Action requires the selection of a file.	Select a file.
No firmware version file was selected.	A file was not selected in the Firmware Library dialog box before an action, such as modify or send was performed.	Click a firmware version in the dialog box to select it, then perform the action again.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed.	Informational message only—no action is required.
Nonredundant director must be offline to install firmware.	For directors, if the director has only one CTP card, the director must be set offline to install a firmware version. For switches, since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Set the director or switch offline and install the firmware.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.
Open Trunking is not installed for this product. Please contact your sales representative.	The Open Trunking feature key has not been enabled. This message is displayed if the optional Open Trunking feature is installed.	Enter the feature key into the Configure Feature Key dialog box and enable the key. If you require a feature key, see your account representative.

Table 31 Element Manager messages (continued)

Message	Description	Action
Performing this operation will change the current state to Offline.	This message requests confirmation to set the director offline.	Click **OK** to set the director offline or click **Cancel** to cancel the operation.
Performing this operation will change the current state to Online.	This message requests confirmation to set the director online.	Click **OK** to set the director online or click **Cancel** to cancel the operation.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the Configure Date and Time dialog box, that the new time or date will overwrite the existing time or date set for the director or switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click **Periodic Date/Time Synchronization** check box in Configure Date and Time dialog box (Configure menu) to clear check mark and disable periodic date/time synchronization.
Port Binding was removed from attached devices that are also participating in Switch Binding.	Informational message. You removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.
Port cannot swap to itself.	Port addresses entered in the Swap Ports dialog box are the same.	Ensure that address in the first and second Port Address boxes are different.
Port diagnostics cannot be performed on an inactive port.	This is displayed when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director speed.	This is displayed when you configure a port to 2 Gb/sec and the director speed is set to 1 Gb/sec.	Set the director speed to 2 Gb/sec in the Configure Switch Parameter dialog box.

Table 31 Element Manager messages (continued)

Message	Description	Action
Port numbers must be in the range of 0 to xxx.	When configuring Preferred Paths, source ports and exit ports must be in the range of ports for the switch being configured.	In the Configure Preferred Paths dialog box, change the numbers in the Source Port and Exit Port boxes to fall within the port count of the switch on which you are configuring paths.
Preferred Paths can not be enabled until the Domain ID is set to Insistent. Disable Preferred Paths, then configure Switch Parameters.	If the switch's domain ID has not been set to Insistent, the user is not allowed to activate the Preferred Path configuration with the Enable Preferred Paths check box selected.	Close the Configure Preferred Paths dialog box and select **Configure > Operating Parameters > Switch Parameters**. In the Configure Switch Parameters dialog box, click the **Insistent** check box.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the Ethernet connection between the HAFM appliance and the director is up or available.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance can be busy. Try the operation again later.
SANtegrity Feature not installed. Please contact your sales representative.	You selected **Switch Binding** from the **Configure** menu, but the optional SANtegrity Binding feature is not installed.	Install the SANtegrity Binding key through the Configure Feature Key dialog box before using Switch Binding features.
Send firmware failed.	A firmware download operation failed.	Retry the firmware download operation. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.

Table 31 Element Manager messages (continued)

Message	Description	Action
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and **Stop** was selected on the Port Diagnostics dialog box. Diagnostics quit for the port for some reason, but the **Stop** button remains enabled.	Verify port operation. Retry diagnostics for the port and choose **Stop** from the dialog box. If problem persists, contact the next level of support.
Stop diagnostics failed. The test was not running.	This action failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the director's Switch Membership List (SANtegrity Binding feature), but you should note that one or more of these devices still has security control in Port Binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the Configure Ports dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switches with failed ports	Replace failed ports.
The add firmware process has been aborted.	You aborted the process to add a firmware version to the HAFM appliance's firmware library.	Verify the firmware addition is to be aborted, then click **OK** to continue.
Switch clock alert mode must be cleared before enabling period synchronization.	Clock alert mode is enabled through the Configure FICON Management Server dialog box and user is attempting to enable Periodic Date/Time Synchronization through the Configure Date and Time dialog box.	Disable clock alert mode through the Configure FICON Management Server dialog box.
The data collection process failed.	An error occurred while performing the data collection procedure.	Try the data collection procedure again. If the problem persists, contact the next level of support.

Table 31 Element Manager messages (continued)

Message	Description	Action
The data collection process has been aborted.	You aborted the data collection procedure.	Verify the data collection procedure is to be aborted, then click **OK** to continue.
The default zone must be disabled to configure.	The message is displayed when you attempted to change the management style to Open Fabric and the default zone is enabled.	Disable the default zone and repeat the operation.
The Ethernet link dropped.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The firmware file is corrupted.	A firmware version file is corrupt.	Contact the next level of support to report the problem.
The firmware version already exists.	This firmware version already exists in HAFM appliance's firmware library.	Informational message only—no action is required.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs.	You attempted to disable these parameters in the Configure Switch Parameters dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box in HAFM, then disable the parameters.
The link to the director is not available.	The Ethernet connection between the HAFM appliance and the director is down or unavailable.	Establish and verify the network connection.
The link to the switch is not available.	The Ethernet connection between the HAFM appliance and the switch is down or unavailable.	Establish and verify the network connection.
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.

Table 31 Element Manager messages (continued)

Message	Description	Action
The management server is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an Element Manager, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.
The optical transceiver is not installed.	Information is not available for a port without an optical transceiver installed.	Install an SFP optical transceiver in the port.
The switch did not accept the request.	The director or switch cannot perform the requested action.	Retry the operation. If the condition persists, contact the next level of support.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.
The switch did not respond in the time allowed.	While waiting to perform a requested action, the director or switch timed out.	Retry the operation. If the condition persists, contact the next level of support.
The switch is busy saving maintenance information.	The director or switch cannot perform the requested action because it is busy saving maintenance information.	Retry the operation later. If the condition persists, contact the next level of support.
The switch must be offline to change the Management Style.	The firmware is below the required level and you attempted to change the management style.	Choose **Set Online State** from the **Maintenance** menu and click **Set Offline**. Then change the management style. Set the director or switch back online when finished.
The switch must be offline to configure.	A configuration changed was attempted for a configuration requiring offline changes.	Take the appropriate actions to set the director or switch offline before attempting the configuration change.
This feature is not installed. Please contact your sales representative.	This feature has not been installed.	Contact your sales representative.

Table 31 Element Manager messages (continued)

Message	Description	Action
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the switch offline through the Set Online State dialog box, then activate the new feature key using the Configure Feature Key dialog box. The new feature key will display both the new features and the features that were installed previously.
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The feature set currently installed for this system contains features that are not being installed with the new feature key.	Click **Yes** to activate the feature key and remove current features not in the new feature set or **No** to cancel.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported on firmware earlier than 01.03.00.	Informational message.
Unable to change incompatible firmware release.	You tried to download a firmware release that is not compatible with the current product configuration.	See the product release notes or contact the next level of support to report the problem.
Unable to save data collection file to destination.	The HAFM appliance could not save the data collection file to the specified location (PC hard drive, CD, or network).	Retry the operation. If the condition persists, contact the next level of support.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.

D Configuring remote workstations

This appendix describes the procedures for installing the HAFM application on a remote workstation. To run HAFM on a remote workstation, you must first download and install the HAFM application from the HAFM appliance.

This appendix describes the following topics:

- Windows systems, page 257
- Solaris systems, page 261
- HP-UX, AIX, and Linux systems, page 263

Windows systems

This section describes the procedures for installing HAFM on a remote workstation running Windows 2000, Windows NT, or Windows XP.

Requirements

The download and installation process requires the use of a PC with the following minimum system requirements:

- Operating system (one of the following):
    - Windows 2000 Professional (with service pack 3 or above)
    - Windows 2003
    - Windows NT 4.0 (with service pack 6a)
    - Windows XP (with service pack 1a)
- 1 GHz Pentium III processor
- 1 GB RAM
- 350 MB available disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Ethernet network adapter
- Java-enabled web browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

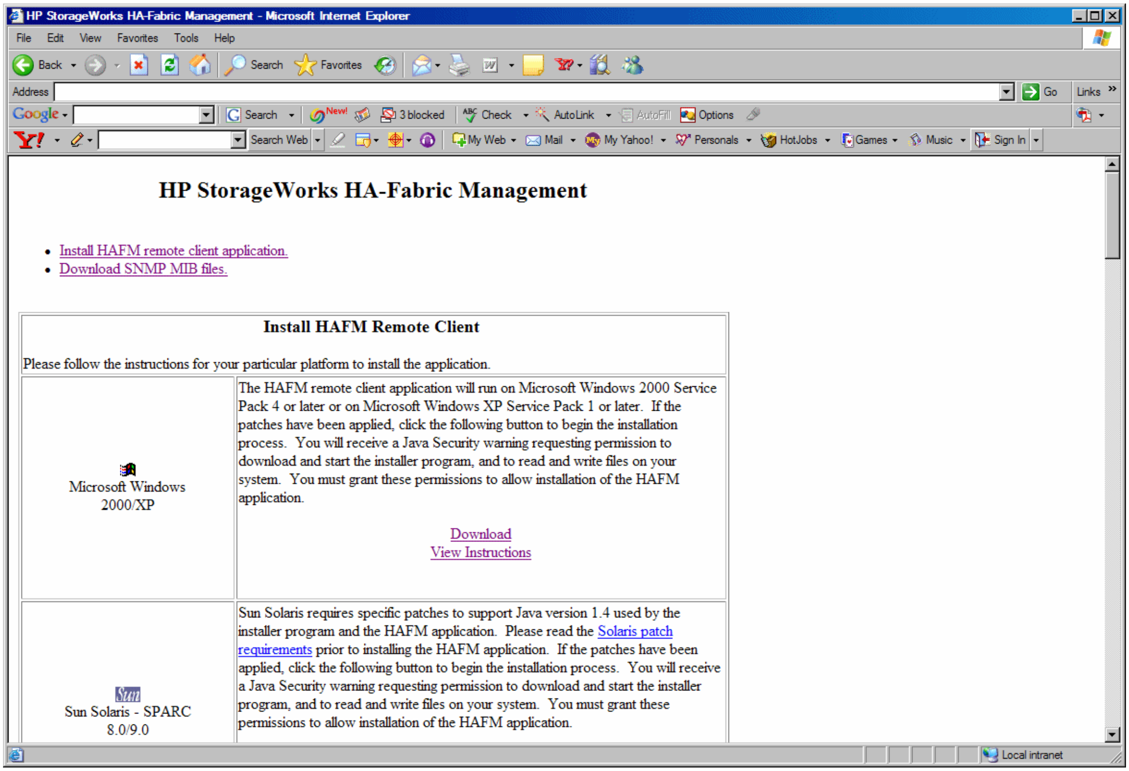
Newer versions of HAFM or Element Managers installed on the HAFM appliance are automatically downloaded when the remote client logs in to the appliance.

Installation procedure

To install HAFM on a remote workstation:

1. Obtain the HAFM appliance address from your network administrator.
2. Open a web browser.
3. Enter the HAFM appliance address in the Location (or Address) box on the browser, and then press **Enter**.

The HP StorageWorks HAFM remote client installation window is displayed. Figure 114 shows the upper portion of this page.



HP StorageWorks HA-Fabric Management

- Install HAFM remote client application.
- Download SNMP MIB files.

Install HAFM Remote Client

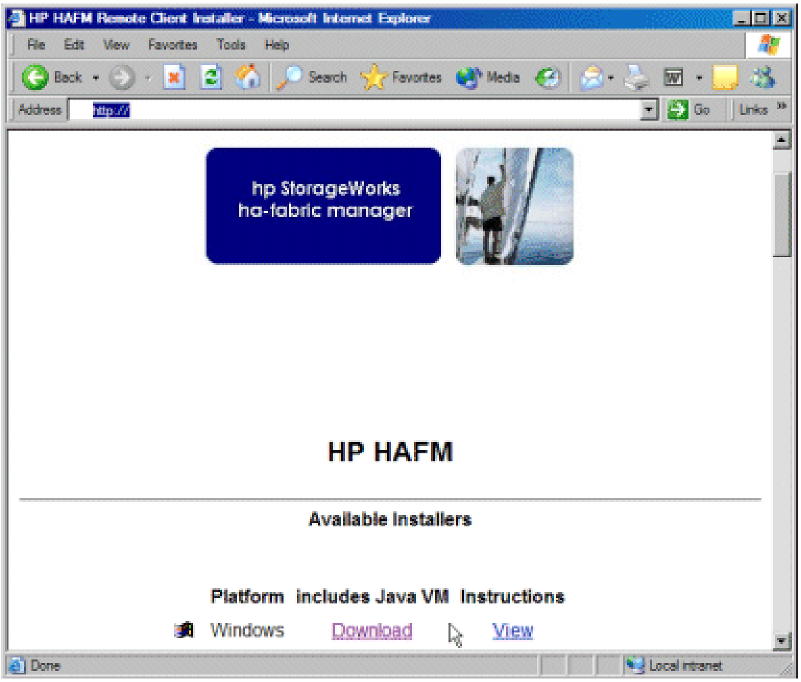
Please follow the instructions for your particular platform to install the application.

Microsoft Windows 2000/XP	The HAFM remote client application will run on Microsoft Windows 2000 Service Pack 4 or later or on Microsoft Windows XP Service Pack 1 or later. If the patches have been applied, click the following button to begin the installation process. You will receive a Java Security warning requesting permission to download and start the installer program, and to read and write files on your system. You must grant these permissions to allow installation of the HAFM application. Download View Instructions
Sun Solaris - SPARC 8.0/9.0	Sun Solaris requires specific patches to support Java version 1.4 used by the installer program and the HAFM application. Please read the Solaris patch requirements prior to installing the HAFM application. If the patches have been applied, click the following button to begin the installation process. You will receive a Java Security warning requesting permission to download and start the installer program, and to read and write files on your system. You must grant these permissions to allow installation of the HAFM application.

Figure 114 Remote client installation page

4. Click **Download** to begin the installation process.
5. If you have read the security agreement information and wish to continue, click **Yes**.

The HP HAFM Available Installers page is displayed (Figure 115).


HP HAFM Remote Client Installer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://
Go Links
hp StorageWorks
ha-fabric manager
Done
Local intranet

HP HAFM

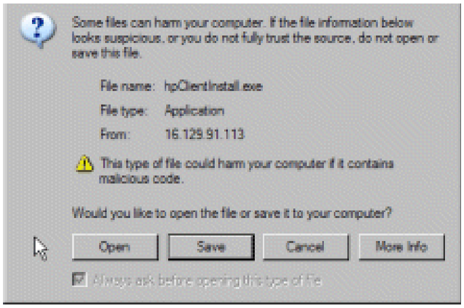
Available Installers

Platform	includes Java VM	Instructions
Windows	Download	View

Figure 115 HP HAFM Available Installers page

6. Click **Download**.

   The File Download dialog box is displayed (Figure 116).



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: hpClientInstall.exe

File type: Application

From: 16.129.91.113

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

Figure 116 File Download dialog box

7. Click **Open**.

   The system begins downloading the HAFM installer. When the download is complete, the Introduction window is displayed.

NOTE: At any time, you can return to the previous page by clicking **Previous** or quit the Installer by clicking **Cancel**.

8. Click **Next**.

   The License Agreement window is displayed.

9. If you have read the license agreement and agree to accept the terms, click I accept the terms of the License Agreement.

10. Click **Next**.

    The Important Information window is displayed.

11. Click **Next**.

    The Choose Install Folder window is displayed.

12. Perform one of the following actions to select a folder on the remote workstation in which to store the HAFM software:

    - Accept the default location.
    - Enter the path to a new location.
    - Click **Choose** to browse for an appropriate location.
    - Click **Restore Default Folder** to change the location back to the default folder.

13. Click **Next**.

14. If HAFM is already installed on the system, you are prompted to uninstall the existing version. If you want to uninstall the existing software, click **Yes** and press **Next**.

15. When the Uninstall HAFM window is displayed, click **Uninstall**.

16. When the Uninstall Complete window is displayed, click **Quit**.

    The Choose Shortcut Location window is displayed.

17. Select a shortcut location. The options for the location of HAFM icons are:

    - In a new Program Group—Adds a new program group on the Start menu for HAFM.
    - In an existing Program Group—Enables you to select from existing program groups on the Start menu for HAFM.
    - In the Start Menu—Puts the HAFM icon on the initial Start menu.
    - On the Desktop—Puts HAFM icons on the Windows desktop.
    - Other—Enables you to choose any location on your hard drive or network for HAFM files.
    - Don't create icons—Prevents the installation from creating an icon for HAFM.

    You can enable the Create Icons for All Users box for some of the shortcut options but not all. If you select the check box, the appropriate HAFM icons are placed on the desktop and in the Programs folder of every Windows user. If you clear the check box, the icons are created only for the current user and are not visible for other user IDs.

18. Click **Next**.

    The Pre-Installation Summary window is displayed.

19. Review the installation information and click **Install**.

The progress of the installation is tracked on the Installing HP StorageWorks HAFM window. When the installation is complete, the Install Complete dialog box is displayed.

20. Click **Done**.

Running HAFM

- If you selected icons to be created in step 17 of the installation procedure, access the icon in the windows Start menu or desktop to run HAFM.
- If you did not create any icons in step 17 of the installation procedure:
  - **a.** Access the HAFM folder (default location: `*Install_Home*/bin/`).
  - **b.** Double-click the file `HAFM_coo.bat` to run HAFM.

Solaris systems

This section describes the procedures for installing HAFM on a remote Solaris workstation.

Requirements

The download and installation process requires the use of a workstation with the following minimum system requirements:

- Solaris version 8 or 9
- UltraSPARC-IIi or greater processor
- 512 MB RAM
- 350 MB available disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Network connection
- Web browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

Newer versions of HAFM or Element Managers installed on the HAFM appliance are automatically downloaded when the remote client logs in to the appliance.

Installation procedure

To install HAFM on a remote workstation:

1. Obtain the HAFM appliance address from your network administrator.
2. Open a web browser.
3. Enter the HAFM appliance address in the Location (or Address) box of the browser, and then press **Enter**.

   The HP StorageWorks HAFM page is displayed.
4. Click **Begin Solaris Installation** to begin the installation process.
5. If you have read the security agreement information and wish to continue, click **Yes**.

   The HP High Availability Fabric Manager Available Installers page is displayed (Figure 115).
6. Click **Download**.

   The File Download dialog box is displayed (Figure 116).

7. Click **Open**.

   The system begins downloading the HAFM installer. When the download is complete, the Introduction window is displayed.

NOTE: At any time, you can return to the previous page by clicking **Previous** or quit the installation by clicking **Exit**.

8. Click **Next**.

   The License Agreement window is displayed.
9. If you have read the license agreement and agree to accept the terms, click I accept the terms of the License Agreement.
10. Click **Next**.

    The Important Information window is displayed.
11. Click **Next**.

    The Choose Install Folder window is displayed.
12. Perform one of the following actions to select a folder on the remote workstation in which to store the HAFM software:
    - Accept the default location.
    - Enter the path to a new location.
    - Click **Choose** to browse for an appropriate location.
    - Click **Restore Default Location** to change the location back to the default.
13. Click **Next**.
14. If HAFM is already installed on the system, you are prompted to uninstall the existing version. If you want to uninstall the existing software, click **Yes** and then click **Next**.
15. When the Uninstall HAFM window is displayed, click **Uninstall**.
16. When the Uninstall Complete window is displayed, click **Quit**.

    The Choose Shortcut Location window is displayed.
17. Select a shortcut location.

    The options for the location of HAFM links are:
    - In your home folder—Adds a new program group on the **Start** menu for HAFM.
    - Other—Enables you to choose any location on your hard drive or network for the HAFM files.
    - Don’t create links—Prevents the installation from creating a link for HAFM.
18. Click **Next**.

    The Pre-Installation Summary window is displayed.
19. Review the installation information and click **Install**.

    The progress of the installation is tracked on the Installing HP StorageWorks HAFM window.
20. If desired, select the Start the High Availability Fabric Manager check box to immediately open HAFM.

21. Click **Done**.

Running HAFM

Run the HAFM program from the directory in which you saved it (the default is a subdirectory named `HAFM` in your home directory).

1. In the Terminal window, enter `cd HAFM`.
2. Press **Enter**.
3. Enter `HAFM_Manager`.
4. Press **Enter**.

   The HAFM application opens.

HP-UX, AIX, and Linux systems

This section describes the procedures for installing the HAFM on a remote HP-UX, AIX, or Linux workstation.

Requirements

The download and installation process requires the use of a PC with the following minimum system requirements:

- Operating system (one of the following):
  - HP-UX 11.0a
  - AIX version 5.1
  - Red Hat 9.0 kernel v.2.4.20-8
  - Red Hat 8.0 kernel v.2.4.18-14
  - Red Hat Enterprise Linux ES 3.0
- Processor:
  - 400 MHz HA PA-RISC
  - 333 MHz Power3-II
  - 1 GHz Intel Pentium III
- 512 MB RAM
- 350 MB disk space
- Video card supporting 256 colors at 800 x 600 resolution
- Ethernet network adapter
- Java-enabled web browser, such as Microsoft Internet Explorer (version 4.0 or later) or Netscape Navigator (version 4.6 or later)

Newer versions of HAFM or Element Managers installed on the HAFM appliance are automatically downloaded when the remote clients log in to the HAFM appliance.

Installation procedure

1. Open a Terminal window by choosing **Terminal** from the Personal Applications subpanel.

2. At the prompt (#), enter `netscape` and then press **Enter**.

   The Netscape browser opens.
3. Obtain the HAFM appliance address from your network administrator.
4. Enter the address of the HAFM appliance in the Location (or Address) box of the browser, and press **Enter**.

   The HP StorageWorks HAFM page is displayed.
5. Read the instructions for your operating system.
6. If a reference to fixes is made, click the hyperlink and verify that your system is up to date.
7. On the HAFM page, click Begin HP-UX Installation/Begin AIX Installation/Begin Linux Installation to begin the installation process.
8. If you have read the security agreement information and wish to continue, click **Yes**.

   The HP High Availability Fabric Manager Available Installers page is displayed (Figure 115).
9. Click **Download**.

   The File Download dialog box is displayed (Figure 116).
10. Click **Open**.

    The system begins downloading the HAFM installer. When the download is complete, the Introduction window is displayed.
11. A Save As dialog box is displayed with the default file name `hpClientInstall.bin`.

    Change the file name to `/home/hpClientInstall.bin`.
12. Click **OK**.

    The software download begins.
13. Close the browser window.
14. In the Terminal window:

    a. Enter `cd home`.

    b. Press **Enter.**

    c. Enter `sh hpClientInstall.bin`.

    d. Press **Enter.**
15. When the download is complete, the Introduction window is displayed.

    Be aware that there can be a considerable delay.
16. Click **Next**.

    The License Agreement window is displayed.

NOTE: At any time, you can return to the previous page by clicking **Previous** or quit the Installation by clicking **Exit**.

17. If you have read the license agreement and agree to accept the terms, click I accept the terms of the License Agreement.
18. Click **Next**.

    The Important Information window is displayed.

19. Click **Next**.

    The Choose Install Folder window is displayed.

20. Perform one of the following to select a folder on the remote workstation in which to store the HAFM software:

    - Accept the default location.
    - Enter the path to a new location.
    - Click **Choose** to browse for an appropriate location.
    - Click **Restore Default Location** to change the location back to the default.

21. Click **Next**.

    If HAFM is already installed on the system, you are prompted to uninstall the existing version. If you want to uninstall the existing software, click **Yes** and then press **Next**.

22. When the Uninstall HAFM window is displayed, click **Uninstall**.
23. When the Uninstall Complete window is displayed, click **Quit**.

    The Choose Shortcut Location window is displayed.

24. Select a shortcut location from this window.

    The options for the location of HAFM links are:

    - **In your home folder**—Adds a new program group on the **Start** menu for the HAFM.
    - **Other**—Enables you to select any location on your hard drive or network for the HAFM files.
    - **Don't create links**—Prevents the installation from creating a link for the HAFM.

25. Click **Next**.

    The Pre-Installation Summary window is displayed.

26. Review the installation information and click **Install**.

    The progress of the installation is tracked on the Installing High Availability Fabric Manager window.

27. If desired, select the Start the High Availability Fabric Manager check box to immediately open the HAFM.
28. Click **Done**.

Running HAFM

Run HAFM from the directory in which you saved it.

1. In the Terminal window, enter `cd HAFM`.
2. Press **Enter**.
3. Enter `./HAFM`.
4. Press **Enter**.

    The HAFM application opens.

E Reference

This appendix provides useful reference information.

Compatibility with other applications

The application is designed to operate smoothly with other enterprise applications and network-monitoring programs. Because this application has fully configurable SNMP trap listening and forwarding functions, it can act as a primary or secondary network manager. It can listen for trap events on any port and can forward traps to other network management software, enabling easy integration into existing systems.

By default, the application is configured to listen for traps on the standard port, 162. Only one software application can control a TCP/IP port at a given time. If the application is not the primary network management tool and you plan to run the application on the same computer, you may need to reconfigure the application to listen for traps on a different port. For instance, if the primary network management software is configured to listen for traps on port 162 and forward them on port 3000, reconfigure the application to listen for traps on port 3000.

Icon legend

Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Physical Map.

Product icons

The following table lists the SAN product icons that display on the topology. Some of the icons shown in Table 32 only display when certain features are licensed. In the case of HP devices, if another appliance is managing a HP device, the Generic HP icon is displayed.

Table 32 Product Icons

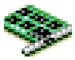
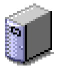
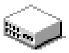
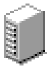
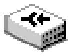
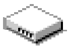
Icon	Description	Icon	Description
	Host Bus Adapter (HBA)		Network Attached Storage (NAS)
	Switch		Storage
	Bridge		Hub

Table 32 Product Icons (continued)

Icon	Description	Icon	Description
?	Unknown		Tape
FCIP	FCIP Bridge Or Gateway		Loop
iSCSI	iSCSI Bridge Or Gateway		Appliance
	HP StorageWorks Edge Switch 2/16		HP StorageWorks Edge Switch 2/32
	HP StorageWorks Edge Switch 2/24		Generic HP StorageWorks switch or director
	HP StorageWorks Director 2/64		HP StorageWorks Director 2/140

Product status icons

Table 33 Product status icons

Icon	Status
No icon	Operational
△	Degraded
♦	Failed
!	Unknown/Offline

Event icons

Table 34 Event icons

Icon	Description
ⓘ	Informational
⚠	Warning
✖	Fatal

Band information status icons

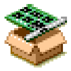
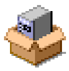
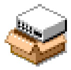
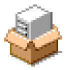
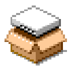
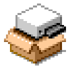
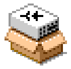
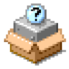
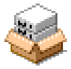
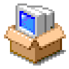
Table 35 Band information status icons

Icon	Out-of-band	In-band	Icon	Out-of-band	In-band
	Present	Not Present		Present	Present
	Failed	Not Present		Present	Failed
	Not Present	Present		Failed	Present
	Not Present	Failed		Failed	Failed

Planned device icons

Icons of planned devices illustrate the device being unpacked from a box. Table 36 illustrates the planned icons for various devices.

Table 36 Planned device icons

Icon	Description	Icon	Description
	Planned Host Bus Adapter (HBA)		Planned Network Attached Storage (NAS)
	Planned switch		Planned storage
	Planned hub		Planned tape
	Planned bridge		Planned unknown device
	Planned JBOD		Planned appliance

Group icons

Table 37 Group icons

Icon	Description	Icon	Description
	Host		Isolated group
	Switch		Bridge
	Loop		Fabric

Connections

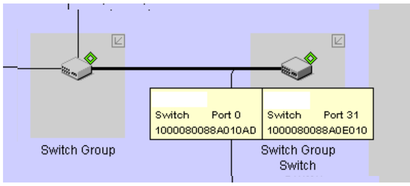


Figure 117 Online connection with online devices

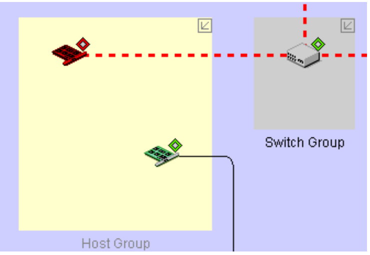


Figure 118 Offline connection and offline loop and storage device

NOTE: In Figure 119, gray lines on the HBA indicate no activity on those connections.

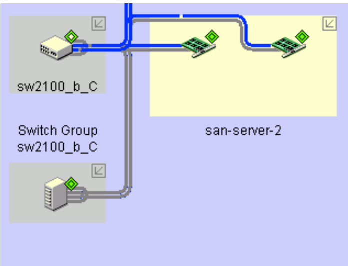


Figure 119 Connection performance as displayed on Physical Map

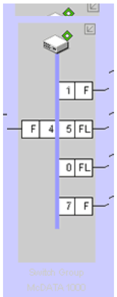


Figure 120 Switch on topology showing ports

Event Management

Event Management enables you to specify triggers and actions to automate tasks. For example, you can set an event trigger to fire at a certain time and day (everyday at noon) and associate the action of sending an e-mail message.

Event trigger properties

This section describes the properties you can set for event triggers.

SNMP trap event properties

SNMP trap events occur when the appliance receives an SNMP trap.

Table 38 describes trap event properties.

Table 38 SNMP trap event properties

Property	Description
IP Address	Device’s IP address
Node Name	Device’s WWN
Port Name	Port’s WWN

Table 38 SNMP trap event properties (continued)

Property	Description
Source	The cause of the event (for example, user ID or device label)
Description	Event description (for example, out-of-band offline)
Event Level	The severity of the event (for example, informational)

Table 39 describes the properties of a device in the SAN.

Table 39 SNMP trap device properties

Property	Description
Label	Device's label, as shown on the Physical Map
Name	Device's name, as specified in the Properties dialog box
Device Type	Type of device (for example, HBA)
Node Name	Device's WWN
IP Address	Device's IP address
Vendor	Device's vendor
Model	Device's model
Serial Number	Device's serial number
Port Count	Device's port count
Firmware	Device's firmware level
Comments	User-entered comments
Text1 through Text4	User-entered values
Device Status	Device's availability (online/offline)

Table 40 describes the properties of the operating system and the appliance.

Table 40 SNMP trap system properties

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN
Client Count	Number of clients logged in to the SAN
Discovery Off	Specifies whether discovery is turned on
Event Notification Off	Specifies whether event notification is turned on
Free Memory	Available physical memory
IP Address	Appliance's IP address
VM Name	Name of the Java Virtual Machine
VM Vendor	Vendor of the Java Virtual Machine
VM Version	Version of the Java Virtual Machine
OS Architecture	Operating system architecture

Table 40 SNMP trap system properties (continued)

Property	Description
OS Name	Operating system name
OS Version	Operating system version
Server Name	Name of the appliance
Subnet Mask	Discovered subnet mask
Total Memory	Total physical memory
Trap Forwarding Off	Specifies whether trap forwarding is enabled
Region	Region of the world where the user is located
Time Zone	User's time zone
User Count	Number of users

Performance event properties

Performance events occur when the performance at a switch port crosses a user-defined threshold.

Table 41 describes the event properties.

Table 41 Performance event properties

Property	Description
Threshold Type	Performance threshold type (for example, high critical)
Measure Type	Performance measurement units
Port Number	Port number that encountered an event
IP Address	IP address of the device that encountered an event
Source	Label of the device where the event occurred
Node Name	WWN of the device that encountered an event
Port Name	WWN of the port that encountered an event
Description	Description of the performance event
Event Level	Severity level

Table 42 describes the properties of a device in the SAN.

Table 42 Performance device properties

Property	Description
Label	Device's label, as shown on the Physical Map
Name	Device's name, as specified in the Properties dialog box
Device Type	Type of device (for example, HBA)
Node Name	Device's WWN
IP Address	Device's IP address
Vendor	Device's vendor

Table 42 Performance device properties (continued)

Property	Description
Model	Device’s model
Serial Number	Device’s serial number
Port Count	Device’s port count
Firmware	Device’s firmware level
Comments	User-entered comments
Text1 through Text4	User-entered values
Device Status	Device’s availability (online/offline)

Table 43 describes the properties of the platform and the appliance.

Table 43 Performance system properties

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN
Client Count	Number of clients logged in to the SAN
Discovery Off	Specifies whether discovery is turned on
Event Notification Off	Specifies whether event notification is turned on
Free Memory	Available physical memory
IP Address	Appliance’s IP address
VM Name	Name of the Java Virtual Machine
VM Vendor	Vendor of the Java Virtual Machine
VM Version	Version of the Java Virtual Machine
OS Architecture	Operating system architecture
OS Name	Operating system name
OS Version	Operating system version
Server Name	Name of the appliance
Subnet Mask	Discovered subnet mask
Total Memory	Total physical memory
Trap Forwarding Off	Specifies whether trap forwarding is enabled
Region	The region of the world where the user is located
Time Zone	User’s time zone
User Count	Number of users

User action event properties

User action events occur when you change a setting in the appliance.

Table 44 describes the user action event properties.

Table 44 User action event properties

Property	Description
Description	Description of the performance event
Source	User ID of the user who performed the action
IP Address	IP address of the client from which the action was taken
Node Name	WWN of the device that encountered an event
Port Name	WWN of the port that encountered an event
Event Level	Severity level of the event (always informational)

Table 45 describes the user action properties about the platform and the appliance.

Table 45 User action system properties

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN
Client Count	Number of clients logged in to the SAN
Discovery Off	Specifies whether discovery is turned on
Event Notification Off	Specifies whether event notification is turned on
Free Memory	Available physical memory
IP Address	Appliance's IP address
VM Name	Name of the Java Virtual Machine
VM Vendor	Vendor of the Java Virtual Machine
VM Version	Version of the Java Virtual Machine
OS Architecture	Operating system architecture
OS Name	Operating system name
OS Version	Operating system version
Server Name	Name of the appliance
Subnet Mask	Discovered subnet mask
Total Memory	Total physical memory
Trap Forwarding Off	Specifies whether trap forwarding is enabled
Region	Region of the world where the user is located
Time Zone	User's time zone
User Count	Number of users

Table 46 describes the properties of a user.

Table 46 User action property

Property	Description
ID	User ID of the user who performed the action
Role	Access level of the user who performed the action (for example, Admin or Browse)
Clients For This User	Number of client sessions open for the specified user

Device state event properties

Device state events occur when a device or connection goes online or offline.

Table 47 describes the properties of a device in a SAN.

Table 47 Device state event properties

Property	Description
Device Status	Status of the device (online or offline)
Discovery Type	In-band or out-of-band discovery
Element Type	A device status event or a link status event
Source	Label of the device that encountered an event
IP Address	IP address of the device that encountered an event
Node Name	WWN of the device that encountered an event
Port Name	WWN of the port that encountered an event
Description	Description of the event
Event Level	Severity level of the event

Table 48 describes the properties about a device in the SAN.

Table 48 Device state properties

Property	Description
Label	Device's label, as shown on the Physical Map
Name	Device's name, as specified in the Properties dialog box
Device Type	Type of device (for example, HBA)
Node Name	Device's WWN
IP Address	Device's IP address
Vendor	Device's vendor
Model	Device's model
Serial Number	Device's serial number
Port Count	Device's port count
Firmware	Device's firmware level

Table 48 Device state properties (continued)

Property	Description
Comments	User-entered comments
Text1 through Text4	User-entered values
Device Status	Device's availability (online/offline)

Table 49 describes the properties about the platform and the appliance.

Table 49 Device state system properties

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN
Client Count	Number of clients logged in to the SAN
Discovery Off	Specifies whether discovery is turned on
Event Notification Off	Specifies whether event notification is turned on
Free Memory	Available physical memory
IP Address	Appliance's IP address
VM Name	Name of the Java Virtual Machine
VM Vendor	Vendor of the Java Virtual Machine
VM Version	Version of the Java Virtual Machine
OS Architecture	Operating system architecture
OS Name	Operating system name
OS Version	Operating system version
Server Name	Name of the appliance
Subnet Mask	Discovered subnet mask
Total Memory	Total physical memory
Trap Forwarding Off	Specifies whether trap forwarding is enabled
Region	Region of the world where the user is located
Time Zone	User's time zone
User Count	Number of users

Writing Event Management macros

You can write macros for Event Management to add relevant data to the action phrases. The following actions allow macros:

- E-mail
- Launch
- Log
- Message

When you right-click near the cursor in a text area, a menu of the context property sets is displayed. Select one of the choices to see a list of the available context properties. Select one of the properties to insert a bracketed macro at the cursor.

When the trigger fires, the values for the context properties that you selected are inserted into the text in place of the macro. Write the text in such a way that you know what the value is since the property name is not inserted along with the value. Example: "`The device labeled ${`*`PROPlabel`*`} has come back online. Its Node Name is ${`*`PROPnodename`*`}`".

NOTE: Actions that are triggered by a schedule trigger do not have access to Device and Event properties since no device is directly involved in triggering the policy.

Table 50 describes event context properties.

Table 50 Event context properties

Property	**Description**
Device Status	Status of the device (online or offline)
Discovery Type	In-band or out-of-band discovery
Element Type	A device status event or a link status event
Threshold Type	Performance threshold type (for example, high critical)
Measure Type	Performance measurement units
Port Number	Port number that encountered an event
IP Address	IP address of the device that encountered an event
Source	Label of the device that encountered an event
Node Name	WWN of the device that encountered an event
Port Name	World-wide name of the port that encountered an event
Description	Description of the event
Event Level	Severity level of the event

Table 51 describes the properties about a device in a SAN.

Table 51 Device context properties

Property	**Description**
Label	Device's label, as shown on the Physical Map
Name	Device's name, as specified in the Device Properties dialog box
Device Type	Type of device (for example, HBA)
Node Name	Device's WWN
IP Address	Device's IP address
Vendor	Device's vendor
Model	Device's model
Serial Number	Device's serial number
Port Count	Device's port count
Firmware	Device's firmware level
Comments	User-entered comments
Text1 through Text4	User-entered values
Device Status	Device's availability (online/offline)

Table 52 describes time context properties.

Table 52 Time context properties

Property	**Description**
mm:dd:hh:mm:ss	Specifies date and time by month, day, hour, minute, and second
hh:mm:ss	Specifies the time by hour, minute, and second
raw	Specifies the time, in milliseconds, since Jan 1, 1970 UTC, for example, 1027966562386
<User-defined>	Format from the Java SimpleDateFormat class; see http://java.sun.com/j2se/1.3/docs/api/ for additional information

Table 53 describes the user context properties.

Table 53 User context properties

Property	Description
ID	The ID of the user who performed the action
Role	The access level of the user who performed the action (for example, Admin or Browse)
Clients for this user	The number of client sessions open for the specified user

Table 54 describes the properties about the platform and the appliance.

Table 54 System context properties

Property	Description
Admin Client Count	Number of administrator clients logged in to the SAN
Client Count	Number of clients logged in to the SAN
Discovery Off	Specifies whether discovery is turned on
Event Notification Off	Specifies whether event notification is turned on
Free Memory	Available physical memory
IP Address	Appliance's IP address
VM Name	Name of the Java Virtual Machine
VM Vendor	Vendor of the Java Virtual Machine
VM Version	Version of the Java Virtual Machine
OS Architecture	Operating system architecture
OS Name	Operating system name
OS Version	Operating system version
Server Name	Name of the appliance
Subnet Mask	Discovered subnet mask
Total Memory	Total physical memory
Trap Forwarding Off	Specifies whether trap forwarding is enabled
Region	Region of the world where the user is located
Time Zone	User's time zone
User Count	Number of users

- **EXEC context property set**—Executes the command that is contained in the macro, and then replaces it with the output of that command.
- **FILE context property set**—Inserts the contents of the file whose path and file name you specify in the macro.

Keyboard shortcuts

You can use the keystrokes shown in Table 55 to perform common functions.

NOTE: To open a menu using keystrokes, press Alt + the underlined letter. To open a submenu, release the Alt key first, then press Shift + the key for the underlined letter of the submenu option.

Table 55 Keyboard shortcuts

Menu item or function	Keyboard shortcut
All Panels	F12
Collapse All	Ctrl-L
Copy	Ctrl-C
Cut	Ctrl-X
Delete	Delete
Delete All	Ctrl-Delete
Expand All	Ctrl-E
Help	F1
Insert Devices	Ctrl-D
New Plan	Ctrl-N
Open Plan	Ctrl-O
Paste	Ctrl-V
Product List	F9
Properties	Ctrl-P
Master Log	F5
Select All	Ctrl-A
Select Connections	Ctrl-T
Event Management	F11
View Selected Device's Ports	F4
View Physical Map	F7
View Utilization Connections	Ctrl-U

F Editing batch files

This appendix provides instructions for updating batch files. It includes:

- Configuring the application to use dual network cards, page 283
- Setting the zoning delay, page 284
- Specifying a host IP address in multi-NIC networks, page 284
- Editing Master Log settings, page 286

Configuring the application to use dual network cards

Issues with client-to-server connectivity can be due to different causes. Some examples are:

- The computer running the application has more than one network card (NIC) installed.
- The computer running the application is behind a firewall that performs network address translation.

In order to ensure that clients can connect to the server, edit the `HAFM_sc.bat` file to manually specify the IP address that the server should communicate to its clients.

Windows systems

1. Open the *`Install_Home`*`\bin\HAFM_sc.bat` file using a text editor.
2. Find the following lines and add the bold text with one space before and after the text:

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Djava.rmi.server.hostname=x.x.x.x -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer -Dsmp.flavor=%APP_FLAVOR%
Server
```

   where **x.x.x.x** is the desired IP address for the appliance.

UNIX systems

1. Open the *`Install_Home`*`/bin/HAFM_Mgrfile` using a text editor (for example, vi).
2. Edit all instances of the following lines:

```
#SMP Server
${SAN_JRE_DIR}/bin/java -classpath ${CLASSPATH}
-Dsmp.deployment.prefix=Server/ -Dsmp.server.edport=%1
-DZoning=Principal com.smp.server.SANMgrRMI
```

to read:

```
#SMP Server
${SAN_JRE_DIR}/bin/java -classpath ${CLASSPATH}
-Dsmp.deployment.prefix=Server/
-Djava.rmi.server.hostname=x.x.x.x
-Dsmp.server.edport=%1 -DZoning=Principal
com.smp.server.SANMgrRMI
```

where **x.x.x.x** is the desired IP address for the server.

Setting the zoning delay

Edit the batch file to set the application to configure zoning through either ECC or Telnet. If a response is not received within the amount of time specified here, the application ends the operation and report that it failed. If the flag is not set, the time-out returns to its default setting of 180000 ms (180 sec).

NOTE: Setting large zones through Telnet can take a long time for large zone sets—approximately six seconds for each zone set.

Windows systems

1. Open the *Install_Home*\bin\HAFM_sc.bat file using a text editor.
2. Find the following lines and add the bold text with one space before and after the text:

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx512m -Xminf.15 -Xmaxf.35
-classpath %CLASSPATH% -Dsmp.Mp.max=512 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer -Dsmp.flavor=%APP_FLAVOR%
Server
```

3. Edit the `-Dsmp.zoning.wait.timeout` entry. Be sure to add a space after your entry.
4. Save and close the file.

Specifying a host IP address in multi-NIC networks

In a network that has two or more NICs, the local host IP returns one of the IPs known to the system. To specify which IP is returned, edit the `Dsmp.server.edipaddress` variable to instruct the Trap Event Distributor to use a specific IP address.

Windows server running as an executable

1. Open the *Install_Home*\bin\HAFM_sc.bat file using a text editor.

2. Edit the following lines:

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
-Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=Principal -Dsmp.zoning.wait.timeout=180000
-Dsmp.webServer -Dsmp.backupManager
-Dsmp.locale.customization=en_US_HAFM Server
```

to read:

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
-Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.server.edipaddress=x,x,x,x -Dsmp.zoning=Principal
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.backupManager
-Dsmp.locale.customization=en_US_HAFM Server
```

where **x.x.x.x** is the desired IP address.

Windows server running as a service

1. Stop the service.
2. Uninstall the service.
3. Edit the following lines in the `install_service.bat` file

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
-Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=Principal -Dsmp.zoning.wait.timeout=180000
-Dsmp.webServer -Dsmp.backupManager
-Dsmp.locale.customization=en_US_HAFM Server
```

to read:

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
-Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.server.edipaddress=x,x,x,x -Dsmp.zoning=Principal
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.backupManager
-Dsmp.locale.customization=en_US_HAFM Server
```

where **x.x.x.x** is the desired IP address.

4. Save the file.
5. Run the `install_service.bat` file.

UNIX systems

1. Open the `Install_Home/bin/HAFM_Mgr` file using a text editor (for example, vi).
2. Edit all instances of the following lines:

   ```
   #SMP Server
   ${SAN_JRE_DIR}/bin/java -classpath ${CLASSPATH}
   -Dsmp.deployment.prefix=Server/ -Dsmp.server.edport=%1
   -DZoning=Principal com.smp.server.SANMgrRMI
   ```

   to read:

   ```
   #SMP Server
   ${SAN_JRE_DIR}/bin/java -classpath ${CLASSPATH}
   -Dsmp.deployment.prefix=Server/
   -Dsmp.server.edipaddress=x,x,x,x -Dsmp.server.edport=%1
   -DZoning=Principal com.smp.server.SANMgrRMI
   ```

   where **x.x.x.x** is the desired IP address.

Editing Master Log settings

The application keeps a log of events that occur in the SAN. By default, the event history will be kept for 45 days, until 50 MB of disk space is taken up, or when the number of entries reaches 2000.

Windows systems

1. Open the `Install_Home\bin\HAFM_sc.bat` file using a text editor (for example, Notepad).
2. Find the following lines:

   ```
   rem HAFM Server
   start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
   -Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
   -Dsmp.Mp.max=128 -Dsmp.autodiscovery=false
   -Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
   -Dsmp.zoning=Principal -Dsmp.zoning.wait.timeout=180000
   -Dsmp.webServer -Dsmp.flavor=HAFM Server
   ```

3. After the `-Dsmp.zoning.wait.timeout` line, add the following lines. Be sure to include a space before and after each entry.
   - `-Dsmp.log.maxLogDiskSpace` (maximum space reserved for the log, between 1MB and 1024MB, inclusive)

- `-Dsmp.log.eventCountAfterTruncate` (number of entries to be saved, between 1 and 2000).

```
rem HAFM Server
start %JAVA_HOME%\bin\HAFMServer.exe -server -Xmx128m
-Xminf.15 -Xmaxf.35 -Xincgc -classpath %CLASSPATH%
-Dsmp.Mp.max=128 -Dsmp.autodiscovery=false
-Dsmp.mpi.test -Dsmp.deployment.prefix=Server/
-Dsmp.zoning=Principal -Dsmp.zoning.wait.timeout=180000
-Dsmp.log.maxLogDiskSpace=50
-Dsmp.log.eventCountAfterTruncate=1000 -Dsmp.webServer
-Dsmp.flavor=HAFM Server
```

UNIX systems

1. Open the *Install_Home*`/bin/HAFM_Mgr` file using a text editor (for example, vi).
2. Find all instances of the following lines:

```
#SMP Server (xmx and smp.Mp.max should agree)
${SAN_JRE_DIR}/bin/java -server -Xmx128m -classpath
${CLASSPATH} -Dsmp.Mp.max=128 -Dsmp.callback.retries=100
-Dsun.java2d.noddraw=true -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=legacy
-Dsmp.zoning.wait.timeout=180000 -Dsmp.webServer
-Dsmp.flavor=%APP_FLAVOR% Server & -Xmaxf.35 -Xincgc
-classpath ${CLASSPATH} -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=Principal
-Dsmp.zoning.wait.timeout=180000 Server
```

   where `%APP_FLAVOR%` is `HAFM`

3. After the `-Dsmp.zoning.wait.timeout line`, add the following lines. Be sure to include a space before and after each entry.
   - `-Dsmp.log.maxLogDiskSpace` (maximum space reserved for the log, between 1MB and 1024MB, inclusive)
   - `-Dsmp.log.eventCountAfterTruncate` (number of entries to be saved, between 1 and 2000).

```
-Xmaxf.35 -Xincgc -classpath ${CLASSPATH} -Dsmp.mpi.test
-Dsmp.deployment.prefix=Server/ -Dsmp.zoning=Principal
-Dsmp.zoning.wait.timeout=180000
-Dsmp.log.maxLogDiskSpace=50
-Dsmp.log.eventCountAfterTruncate=1000 Server &
```

Index